FrontDoor Release 6

The Manual

©Tightrope Media Systems

User Manual for FrontDoor 6.0.0 Build 124

Printed September 8, 2015

Contents

1 Introduction **7**
- 1.1 Welcome to FrontDoor! . . . 7
- 1.2 About Tightrope . . . 7

2 FrontDoor: The Gatekeeper **9**
- 2.1 What Is FrontDoor? . . . 9
  - 2.1.1 User Management . . . 9
  - 2.1.2 Server Setup . . . 9
- 2.2 The Language of FrontDoor . . . 9

I User Management **11**

3 User Management Basics **13**
- 3.1 Users . . . 13
- 3.2 Access Rights . . . 13
- 3.3 Roles . . . 14
- 3.4 Domains . . . 17
- 3.5 A Recap... . . . 18

4 Application Specifics **19**
- 4.1 Things to Consider for Carousel . . . 19
  - 4.1.1 Carousel Access . . . 19
  - 4.1.2 Domains: Zones and Zone Tags . . . 19
  - 4.1.3 User Account Limitations . . . 21
- 4.2 Things to Consider for Cablecast . . . 21
  - 4.2.1 Cablecast Access . . . 21
  - 4.2.2 Domains: Locations and Channels . . . 21
- 4.3 Things to Consider for FrontDoor . . . 24
  - 4.3.1 FrontDoor Access . . . 24
  - 4.3.2 Domains: Where'd they go!? . . . 24

5 A Walk-through: Creating Users With a Purpose **25**
- 5.1 Step 0: Logging in . . . 25
- 5.2 Step 1: Create Roles . . . 26
- 5.3 Step 2: Create Users . . . 30
- 5.4 Step 3: Assigning Roles . . . 32
- 5.5 Day to Day Tasks . . . 36
  - 5.5.1 Updating User Information . . . 36
  - 5.5.2 Deleting Users . . . 37
  - 5.5.3 Resetting User Passwords . . . 37
  - 5.5.4 Unlocking User Accounts . . . 37
  - 5.5.5 Changing Passwords . . . 38

II Server Setup 41

6 Introduction to Setting Up Your Server 43
6.1 An Overview of Server Setup . . . 43
6.1.1 Site Name . . . 43
6.1.2 Site Login Url . . . 43
6.1.3 Server Security . . . 43
6.1.4 Mail Settings . . . 45
6.1.5 Time Settings . . . 45
6.1.6 Licensing . . . 45
6.1.7 Updates . . . 45
6.1.8 Database Tools . . . 45
6.1.9 Privacy Policy . . . 45
6.1.10 About . . . 46
6.2 Important Things to Set Up . . . 46

7 Server Setup Reference 47
7.1 Site Name . . . 47
7.2 Site Login Url . . . 47
7.3 Server Security . . . 48
7.4 Mail Settings . . . 48
7.5 Time Settings . . . 50
7.5.1 Tightrope Time Synchronization . . . 50
7.5.2 Windows Time Synchronization . . . 50
7.5.3 Domain Controller Time Synchronization . . . 51
7.5.4 No Time Synchronization . . . 52
7.6 Licensing . . . 52
7.6.1 Setting a New License Key . . . 53
7.6.2 Confirming a New License Key . . . 54
7.7 Updates . . . 55
7.7.1 Selecting Updates for Download . . . 55
7.8 Database Tools . . . 56
7.9 Privacy Policy . . . 58
7.10 About . . . 58

III Appendix 61

A Access Rights Reference 63
A.1 Access Rights In FrontDoor . . . 63
A.1.1 Server Setup . . . 63
A.1.2 User Management . . . 63
A.2 Access Rights In Carousel . . . 63
A.2.1 Create - Standard Bulletins . . . 63
A.2.2 Create - Uploaded Bulletins . . . 63
A.2.3 Create - Dynamic Bulletins . . . 63
A.2.4 Create - Interactive Bulletins . . . 63
A.2.5 Create - Alert Bulletins . . . 63
A.2.6 Create - Repeating Bulletins . . . 64
A.2.7 Create - Set Extra Bulletin Properties . . . 64
A.2.8 Create - Submit Bulletins to this Zone . . . 64
A.2.9 Create - Template Quick Edit . . . 64

A.2.10 Create - Auto Authorize Bulletins . . . 64
A.2.11 Manage - All Bulletins . . . 64
A.2.12 Manage - Approve Waiting Bulletins . . . 64
A.2.13 Manage - Bulletin Housekeeping . . . 64
A.2.14 Manage - Other User Bulletins . . . 64
A.2.15 Media - Manage User Media . . . 64
A.2.16 Media - Manage Zone Media . . . 64
A.2.17 Media - Edit Bulletin Templates . . . 64
A.2.18 Setup - Zone Setup . . . 65
A.2.19 Setup - Global System Configuration . . . 65
A.2.20 Other - Extras . . . 65
A.2.21 Other - Edit EventDisplay Schedule . . . 65
A.3 Access Rights In Cablecast . . . 65
A.3.1 Modify Schedule (Location or Channel based) . . . 65
A.3.2 Modify Crawl Schedule (Location or Channel based) . . . 65
A.3.3 Modify Shows (Location based) . . . 65
A.3.4 Autopilot Force (Location based) . . . 65
A.3.5 Autopilot Send (Location based) . . . 65
A.3.6 Modify Location Settings (Location based) . . . 65
A.3.7 Modify System Settings (Global) . . . 65
A.3.8 Plugin Access (Global) . . . 66
A.3.9 Reporting Access (Global) . . . 66
A.3.10 Batch Functions (Location based) . . . 66

B Active Directory Integration **67**
B.1 Overview of Setup . . . 67
B.2 Join the Carousel server to the domain . . . 67
B.3 Run the web server and application pool as a user account . . . 67
B.4 Create Active Directory groups . . . 68
B.5 Modify the FrontDoor Web.config file . . . 68
B.6 Modify the Carousel Web.config file . . . 69
B.7 Log into FrontDoor . . . 69
B.8 Notes on how we integrate with Active Directory . . . 69

C Network Ports **71**
C.1 Outgoing Ports . . . 71
C.2 Incoming Ports . . . 71

D Troubleshooting **73**
D.1 Why can't my users can't log in? . . . 73
D.2 I can't log in with the Admin account . . . 73
D.3 Why can't my users access Cablecast? . . . 73
D.4 Why can't my users access Carousel? . . . 73
D.5 My server's time drifts. . . . 73
D.6 I don't have access to an email server. . . . 74

E Release History **75**
E.1 Frontdoor 6.0.0 Release Notes . . . 75

1 Introduction

1.1 Welcome to FrontDoor!

Thank you for purchasing FrontDoor from Tightrope Media Systems. This guide is designed to help administrators through the process of setting up a FrontDoor server. For specific information about Carousel or Cablecast, please see their respective manuals.

1.2 About Tightrope

Tightrope Media Systems is a manufacturer of broadcast and digital signage systems. We are the best at developing whole product solutions that deliver a tailored experience and fantastic utility for our customers.

For more information on Tightrope Media Systems, please visit our web site: www.trms.com

Email us at: sales@trms.com

Our Address is:

Tightrope Media Systems
800 Transfer Road, Suite 1B
Saint Paul, Minnesota 55114

For customer service, please contact your dealer or Tightrope Media Systems directly:

Email : support@trms.com

Online Documentation : www.trms.com/support/documentation

Training Videos : www.trms.com/support/training

Blogs : blog.trms.com

Community Forum : http://getsatisfaction.com/trms

Phone : (866) 866-4118 / (612) 866-4118

The fastest way to get support is through email or the online support form. The community forum is a great place to share tips and tricks, too.

Throughout this guide, the following conventions will be used:

This is a note. Notes are used to call attention to special information that may be helpful to keep in mind.

This is a tip. Tips show unique ways to use the software, and tricks that have been picked up by other users.

This is a warning. Warnings call attention to actions that may result in unforeseen consequences, such as actions that delete large amounts of data or configurations that might have network security implications.

This is a margin note.

If we want to highlight a section of the text that is critical to a particular topic, we'll insert a margin note, like the one you see next to this paragraph. Margin notes might also include small pictures of the user interface, when a figure would be too cumbersome.

! → If we need to call special attention to something that is critical, you might see the symbol that you now see to the left.

When the text references a particular menu item, field or label within the software, that text will appear as follows:

Example: Click on the **Record** button.

When we talk about or reference a menu in the software, we use a special style and reference it in the margin. When we reference menus, we leave out the main menu and we separate each menu with a colon (":").

View: Preferences…: Channels

Example: To change your channels' names, go to *View: Preferences…: Channels*.

When the text references user input, "`this format`" will appear.

Example: Enter "`1234`" into the number field.

When quotes are used to display user input, do not include them in your input unless specifically told to do so.

You'll notice that we've used a couple of 'Examples:' in this section. You will see those throughout the text. They highlight…examples.

2 FrontDoor: The Gatekeeper

2.1 What Is FrontDoor?

FrontDoor acts as the gatekeeper to your Tightrope Media Systems server. It's the first thing you see when you access the server, and it ensures that you're only allowed to do what you've been given permission to do. Most users will only have a fleeting experience with FrontDoor. They'll use it to log in, maybe change their password, then immediately continue on to other applications, like Carousel or Cablecast. Administrators, however, will dive much deeper into FrontDoor, using it to shape what their users can see or do within Carousel or Cablecast.

FrontDoor plays two important parts in the Tightrope system: User Management and Server Setup.

2.1.1 User Management

Primarily, FrontDoor acts as a "single sign-on" application for Tightrope web-applications. This means that anyone who wants to use Carousel or Cablecast must first log-in through FrontDoor. To this end, FrontDoor is responsible for keeping track of who gets to use the applications, and to what extent. More information about User Management can be found in chapter 3 on page 13.

2.1.2 Server Setup

FrontDoor also maintains a set of configuration options that affect the entire system. For example, settings for synching the system clock are found in FrontDoor, because it would be silly change those settings in *both* Carousel and Cablecast. More information about Server Setup can be found in chapter 6 on page 43.

2.2 The Language of FrontDoor

As you read this manual, knowing the following terms will come in handy. We'll only take a brief look at them now, as they will be defined more completely in the coming chapters.

User : Someone who can log in to FrontDoor. May refer to either the "flesh and blood" person who is using the system, or the software account they are using to log in.

Account : Synonym for *User*, specifically the software-based account.

Role : *Users* of the system may have several different areas for which they are responsible. We refer to an area of responsibility as a user's *Role*. *Users* can have many *Roles*.

Access Right : A *Role* is comprised of a set of one or more *Access Rights*. They are the building blocks that define a discrete area of responsibility.

Permission : Synonym for *Access Right*.

Domain : The scope to which a *Role* is applicable for a *User*. This is a complex concept that is defined in-depth later.

Access Domain : Synonym for *Domain*.

Server : The physical computer that hosts FrontDoor. May also host a combination of Carousel and/or Cablecast.

System : Synonym for *Server*.

Carousel : Tightrope Media System's digital signage application. *Users* are given access to Carousel by assigning them a Carousel *Role* in FrontDoor.

Cablecast : Tightrope Media System's broadcast automation application. *Users* are given access to Cablecast by assigning them a Cablecast *Role* in FrontDoor.

Web-Application : A generic term for either FrontDoor, Carousel, or Cablecast. Specifically, the web sites associated with each.

I. User Management

3 User Management Basics

In this chapter, we'll go over the basics of how FrontDoor manages user accounts. We'll begin by first describing some key concepts, then we'll point out some exceptions in Carousel and Cablecast. We will take you on a walk-through of the entire user management process starting in chapter 5 on page 25.

3.1 Users

Tightrope servers support multiple users. A rather bland statement, but a powerful idea. A system which requires a full-time staff person for support and maintenance isn't very economical or practical. FrontDoor allows you to decentralize your efforts by creating several[1] users of the system.

Although having multiple users is handy, too many cooks can spoil the broth. If every user can change every setting in the software, chaos is not far away. To prevent a free-for-all, each user can be given a specific set of responsibilities, while at the same time excluding access to other areas in the software. (See "Access Rights" in section 3.2 and "Roles" in section 3.3 on the next page for more info.)

The default admin login is "Admin" with a password of "trms"

! →

FrontDoor has a special user account built-in: Admin. This account has all access to all areas of all software and cannot be deleted. Anyone possessing the Admin account can do anything he or she pleases in the software. Therefore it is extremely important that access to this account be strictly controlled. Only give the Admin login information to those who need full control of the system.

It is considered a best practice to give yourself a separate user account, and log in as Admin only when needed. This way, if your account is somehow compromised, the Admin account is still safe.

Each and every Tightrope system ships with the same default Admin password of "`trms`". Be sure to change this password immediately!

3.2 Access Rights

Each Tightrope application contains distinct functions or abilities which can be granted to users. These abilities are called Access Rights. If a user has been granted a particular Access Right, he or she will be able to perform that particular ability.

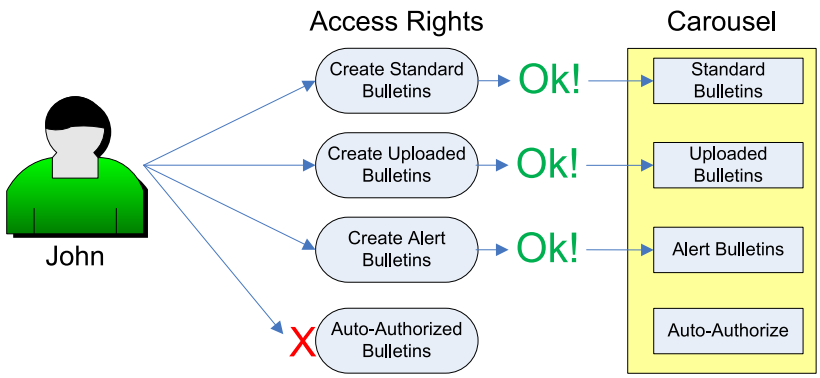
Example: For those who like logic, here's a syllogism. Carousel contains an Access Right which grants the ability to create standard bulletins. If John has a user account on the server which has been granted that Access Right, then John can create standard bulletins using his account[2].

[1] Certain configurations of Carousel limit the number of users you can create. See section 4.1.3 on page 21 for more information.

[2] Actually, this depends on the Domain (scope) to which John has the Access Right. See section 4.1.3 on page 21 for details.

Example: For those who are visual, see figure 3.1. John has a user account on a Carousel system. John's account has the Access Rights related to creating bulletins in Carousel, but isn't allowed access to the other areas of the software.

FIGURE 3.1: A high-level look at Access Rights.



Access Rights are predefined within the software, so you cannot add or delete them, or change the functionality to which they apply. This is by design. But do not despair! Immense customization and flexibility can be achieved by using "Roles," described in section 3.3.

For a list of Access Rights and a description of what they do in each application, see chapter A on page 63.

3.3 Roles

A set of one or more Access Rights can be combined into a Role. This is where it starts to get interesting[3].

Let's say that your Carousel system has two users, John and Scott. From working with both of them in the past, you know that John isn't really one for details, and often gets his facts wrong. Scott, on the other hand is meticulous beyond words, and proofreads every email three times before he sends it. Both John and Scott want to create messages in Carousel, and your job is to give them access. What do you do?

Ideally, you would assign both of them all of the Access Rights related to creating bulletins, but assign the **Auto Approve Bulletins** Access Right only to Scott. With this setup, they both could create bulletins, but John's bulletins would be held for approval before going live, and Scott's bulletins would go live immediately.

We won't go into exactly what each Access Right means for now. For a more complete description of the Access Rights in each application, see chapter A on page 63.

This works fairly well for two users, but imagine if you hired ten more people, half of which were "John-like," and half were "Scott-like." Even in this contrived example, you would end up manually assigning dozens of Access Rights. Multiply the problem by the actual number of Access Rights available in each application,

[3] Although, I guess it depends on your definition of "interesting."

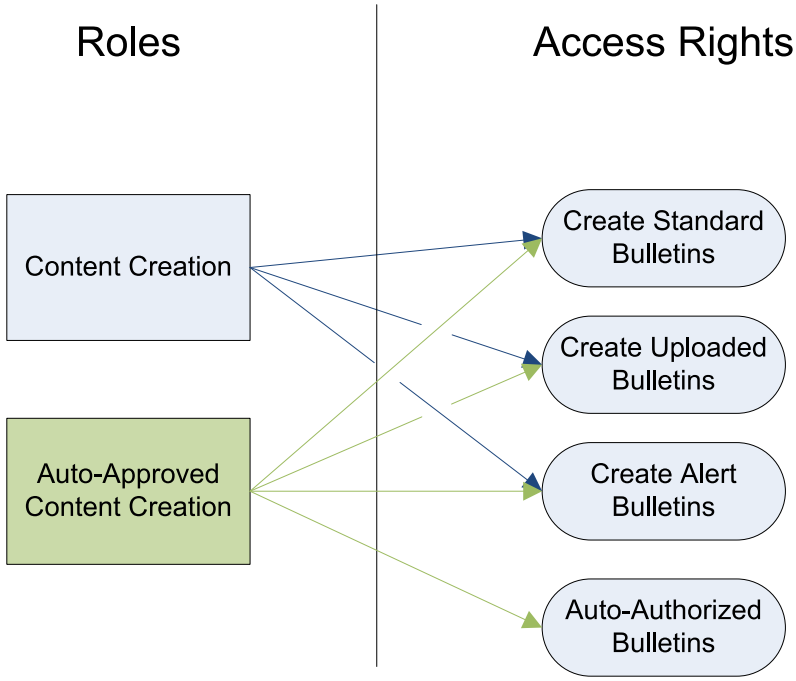
and you'll quickly realize that keeping everything organized would be a challenge even for Scott himself!

Access Rights can be combined into Roles.

Fortunately, FrontDoor solves this problem by abstracting sets of Access Rights into *Roles*. A Role is simply a group of Access Rights. In FrontDoor, you never actually assign Access Rights directly to users. Instead, you first group Access Rights into Roles, and then assign Roles to users.

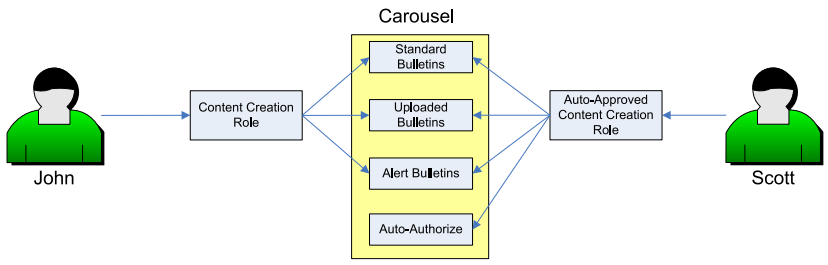
Example: In figure 3.2, we have created two roles, each with a set of Access Rights. The **Content Creation** role contains Access Rights associated with creating bulletins. The **Auto-Approved Content Creation** role contains the same rights as **Content Creation**, plus an additional Access Right allowing for the bulletins to be automatically approved.

FIGURE 3.2: Roles contain Access Rights.



Example: If we consider John and Scott once again, we would assign John the **Content Creation** role, and Scott would get the **Auto-Approved Content Creation Role** as in figure 3.3.

FIGURE 3.3: John and Scott, assigned to their respective Roles.



Unlike Access Rights, you can create any number of Roles in each application. Carousel, for example, ships with a set of default Roles already set up. If they don't quite work for your specific installation, you can modify them, delete them, or add brand new Roles. See section 5.2 on page 26 for details.

Example: After seeing the awesome content that Scott and John are making, Pete comes to you wanting access to Carousel as well. Pete is one of your "Scott-like" detail-oriented employees, so you're fine with having his bulletins automatically approved. You know, however, that Pete likes to play with every whiz-bang feature available. Ideally, you'd like to restrict him to just creating the "Standard" set of bulletins so he doesn't get too wild and crazy. How can we do this?

Initially, you might consider giving Pete the **Auto-Approved Content Creation** Role so his bulletins get automatically approved just like Scott. If you take a look back to figure 3.2 on the preceding page, however, that Role contains Access Rights for all kinds of bulletins, not just the standard type. Giving Pete this role would let him create every kind of bulletin, which you don't want to do.

In this case, you'll need to create a brand new role, something like **Auto-Approved Standard Bulletin Creation**, as in figure 3.4

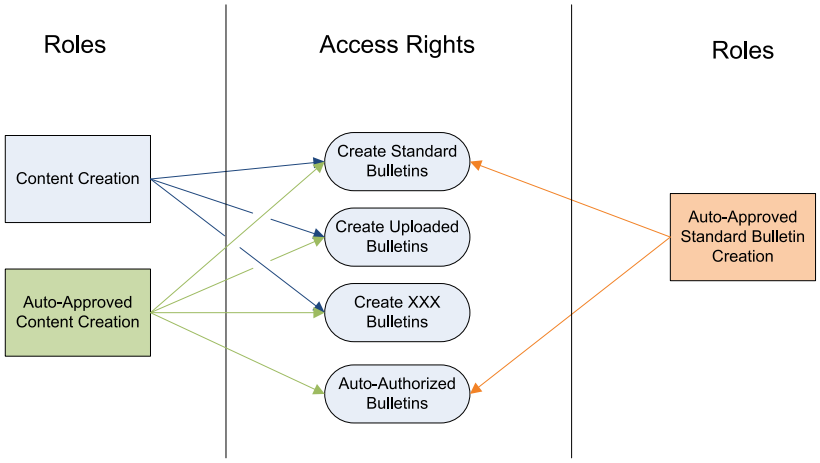


FIGURE 3.4: A new, more specific Role for Pete.

Roles are additive.

You should keep one thing in mind about Roles. They assign Access Rights to users *additively*. This means that a user takes on the *total set* of Access Rights inside each of his or her assigned Roles.

Example: What happens if you gave Pete the **Auto-Approved Standard Bulletin Creation** Role, *and* the **Content Creation** Role? To find out, count up the Access Rights included in those two Roles. As it turns out, giving Pete these two Roles effectively gives him every Access Right.

When determining the Access Rights that a user has, the software takes the union of *all* Access Rights contained in that user's roles.

The drawback here is that no matter how you set up your Roles, you can't give Pete auto-approval for standard bulletins while at the same time denying auto-approval for uploaded bulletins. If Pete has a Role with the auto-approval Access Right, then he has auto-approval period.

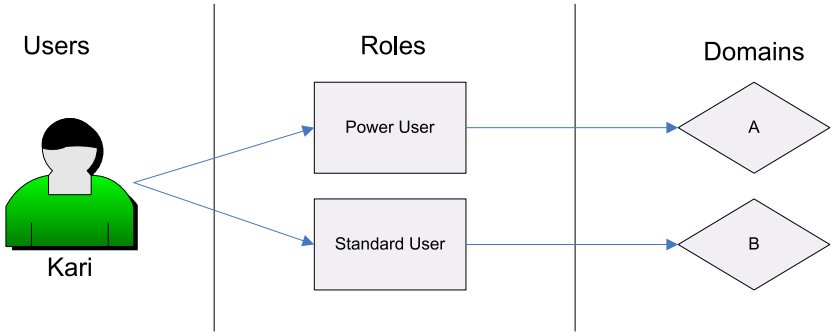
We will step through the process of creating Roles in chapter 5 on page 25.

3.4 Domains

Roles are assigned to Users for a Domain in the software. There's one final twist: Roles have scope. We call this scope a *Domain*. When you are assigning a Role to a user, you must also specify the Domain under which that Role applies.

Example: Kari has an account with two Roles: "Power User" and "Standard User." Each Role has been assigned under a different Domain. As seen in figure 3.5, her role as "Power User" applies under Domain A, whereas "Standard User" applies under Domain B.

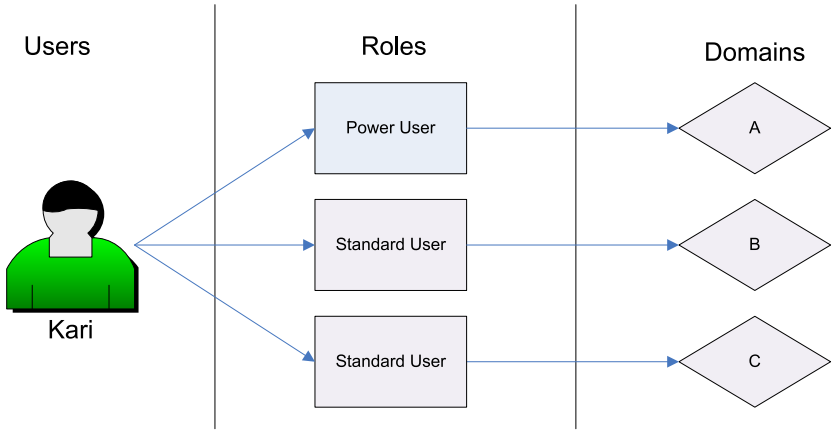
FIGURE 3.5: Kari has two roles, each for different domains.



What this means is that whenever Kari is in Domain B, she's a Standard User. The moment she switches to Domain A, she becomes a Power User, with a new set of Access Rights. Switching back to Domain B relegates her once again to Standard User, with her original set of Access Rights.

Example: If Kari should be a Standard User for multiple domains (say, Domain B *and* Domain C), then she actually gets assigned the "Standard User" Role once again, this time under Domain C as in figure 3.6.

FIGURE 3.6: Kari's two roles, assigned under three different Domains.



Each Tightrope web-application defines its own set of Domains. Descriptions of Domains for FrontDoor can be found in section 4.3.2 on page 24, Carousel in section 4.1.2 on the facing page, and Cablecast in section 4.2.2 on page 21.

3.5 A Recap...

Let's take a quick look at these concepts one more time.

- Tightrope servers support multiple users.
- Each Tightrope application contains distinct functions or abilities (Access Rights) which can be granted to users.
- A set of one or more Access Rights can be combined into a Role.
- Roles are assigned to Users for a Domain in the software.

We put all of these concepts to use in chapter 5 on page 25.

4 Application Specifics

Each Tightrope web-application has some unique features when it comes to User Management. In this chapter, we'll take a look at how Carousel, Cablecast, and FrontDoor differ.

4.1 Things to Consider for Carousel

4.1.1 Carousel Access

In order for your users to access Carousel in any way, they must first be assigned at least one Carousel Role. If you have not given any Carousel Roles to a user, then he or she will not see a link to the Carousel application when they log in to FrontDoor. For more information about Roles, see section 3.3 on page 14. For a look at creating Roles, see section 5.2 on page 26.

4.1.2 Domains: Zones and Zone Tags

Carousel has two domains to which roles can be applied: Zones and Zone Tags.

For details about Zones and Zone Tags, see *Carousel: The Manual*.

A **Zone** corresponds to an area of content within Carousel.

Example: Your Carousel system could have a zone with weather information, another with traffic information, another with event schedules, another with general announcements, etc.

Zone Tags act as keywords for a grouping of Zones. They are formed by adding sets of "Tags" to specific Zones in Carousel. By assigning several Zones the same Zone Tag, they can all be referenced via the Zone Tag.

Example: Let's say you're running a Carousel system for a local university. The campus is divided into two areas: East Campus and West Campus. You can assign a Zone Tag "East Campus" to all Zones that have content specific to the East Campus, and likewise for the West Campus.

What does this mean for FrontDoor? Remember that Roles are assigned for a Domain. Therefore, you can assign a Role in Carousel to be active under a Zone or a Zone Tag. Let's have John and Scott illustrate with their brand new jobs at the aforementioned local university.

Example: Scott is working for the Linguistics department on the West Campus. Being the diligent worker that he is, Scott has been given an "Admin Access" role (which, presumably, gives him all the available Access Rights in Carousel). Scott's kingdom, however, is located only on the West Campus. Therefore, his "Admin Access" role is assigned for the "West Campus" Zone Tag (as seen in figure 4.1 on the next page).

! →

Since the domain for his role is a Zone Tag, this means that Scott has Admin Access *for any Zone tagged with "West Campus."*

Example: John is working in the Computer Science department on the East Campus. John needs to create bulletins for all Zones on the East Campus, so he has a "Content Creation" role for the "East Campus" Zone Tag. He can now create content for any Zone tagged with "East Campus."

Additionally, John is in charge of all the computer labs on the 4th floor of the Electrical Engineering and Computer Science (EECS) building. He likes to make several bulletins a day with tips and tricks for the lab users. Unfortunately, it becomes a major pain to have to wait for an administrator to approve his bulletins each and every time he creates one. Therefore, we've given him an "Auto-Approved Content Creation" role that is assigned to a *single Zone*; the one for the 4th floor in the EECS building.

A Role assigned to a *Zone* is valid for that Zone only.

! → So, John can create content for any Zone tagged with "East Campus." He can also create content that is automatically approved, but *only within the one "EECS 4th Floor" Zone.* This entire situation is pictured in figure 4.1.

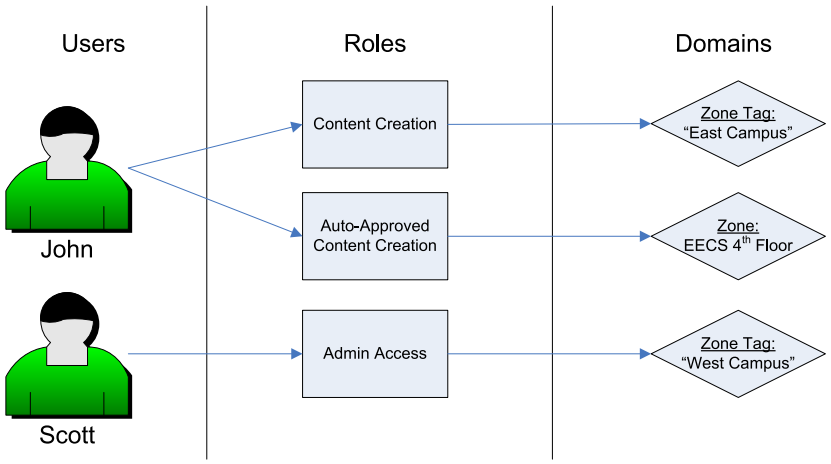


FIGURE 4.1: John and Scott, assigned to different Roles in different Domains.

Zone Tags have an interesting feature. As you add more Zones to a Zone Tag, any Roles assigned to that Zone Tag domain automatically become aware of the new Zone, with no further work from you. In this way, Zone Tags are considered "dynamic."

Example: At the university, you have dozens of users with myriad roles. Every user who needs access to East Campus Zones has their roles assigned under the domain of the "East Campus" Zone Tag. One day, you decide to create a new Zone relating to events at the student union, which is located on the East Campus. In an unfair world, you would now have to edit everyone's Roles, to make them aware of the new Zone. Thankfully, you live in a happy world in which you purchased a Tightrope system[1]. In Carousel, simply add the "East Campus" tag[2] to the new Student Union Zone. Now, any user who has a Role for the "East Campus" Zone Tag automatically has that Role for the Student Union Zone. No changes had to be made in FrontDoor.

A Role assigned to a *Zone Tag* is valid for every Zone that has the tag.

[1] Thanks again, by the way.
[2] See the Carousel manual for info on adding tags to zones.

A best practice is to always assign Carousel roles to a Zone Tag. This should give you the most flexibility when adding new Zones in the future. Assigning a single Zone is more of an exceptional event, as when we gave John a specialized Role for the one Zone in his charge.

4.1.3 User Account Limitations

Certain Carousel systems have limitations on how many user accounts you can create. Every Carousel system will include an Admin account.

- The Carousel Solo line allows you to create a single named user, for a grand total of two user accounts (including the Admin account).
- Carousel Server, Pro, and Enterprise systems allow for an unlimited number of user accounts to be created.
- There are no limitations on the number of Roles you can create.

4.2 Things to Consider for Cablecast

4.2.1 Cablecast Access

In order for your users to access Cablecast in any way, they must first be assigned at least one Cablecast Role. If you have not given any Cablecast Roles to a user, then he or she will not see a link to the Cablecast application when they log in to FrontDoor. For more information about Roles, see section 3.3 on page 14. For a look at creating Roles, see section 5.2 on page 26.

4.2.2 Domains: Locations and Channels

Cablecast has two explicit domains; Locations and Channels. There's also a third, implicit "global" Domain. This sounds a bit confusing, so let's take it one step at a time.

For more information about Channels and Locations, see *Cablecast: The Manual*.

Most cable access stations have a single **Location**. Larger stations may have multiple Locations. Cablecast Roles can be assigned to any particular Location Domain.

Consider a station (TRMS-TV) that has two locations: a main "Head-end" location, and a second "Satellite" location in the next city. We've created a Cablecast Role called "Show Modification" which allows users to edit show records. Recall that all Roles are assigned for a Domain. Let's look at how to assign this role with the help of John and Scott once again.

Example: Scott works at the Head-end, and he keeps track of almost all of the shows for TRMS-TV. John works at the Satellite location, and is in charge of a handful of shows that are housed there. To keep John from messing around with Scott's Head-end shows, we assign John the Show Modification Role for the Satellite Location Domain. Scott, on the other hand, gets the role for his Head-end Location, as pictured in figure 4.2 on the next page.

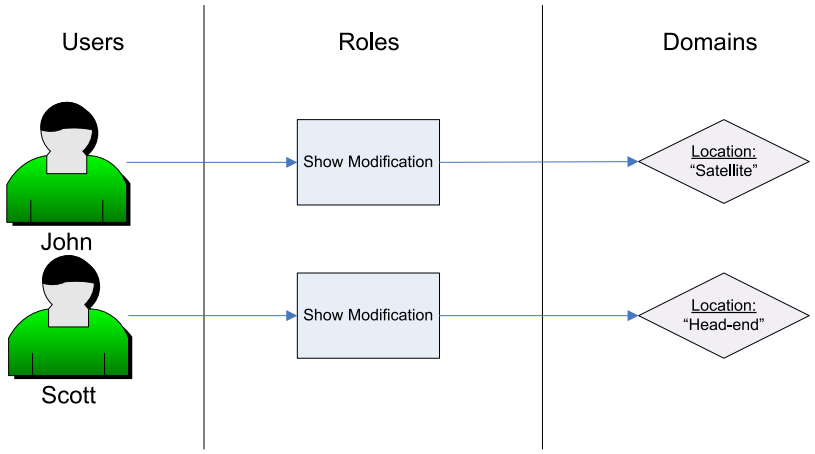


FIGURE 4.2: John and Scott, assigned to different Roles in different Domains.

Things get a bit more complex when we talk about **Channels**, the next type of Domain in Cablecast. Each Location can have one or more Channels, and every Channel has a Schedule of programs to be played on air.

This time, let's say TRMS-TV has a single location, "Head-end." The Head-end Location has two Channels, "Pub-15" and "Gov-16." The Public channel schedules shows that are produced by members of the community, whereas the Government channel plays city council meetings, school board meetings, etc.

Example: You've got two staffers working at TRMS-TV; Pete and Kari. Pete's in charge of Gov-16 programming, and Kari runs programming on Pub-15. Ideally, you'd like to prevent Pete from scheduling shows on Kari's channel, and vice versa. This can be accomplished by creating a "Scheduling" Role in Cablecast, and assigning it Pete and Kari for their respective Channel Domains, as in figure 4.3 on the facing page.

We see Scott in figure 4.3 too, and he's got the Scheduling role assigned to him for the entire Head-end Location. To understand what happens with Scott in this case, we need to dive a little deeper.

! → Here comes the complex part. Remember Access Rights, mentioned first in section 3.2 on page 13? In Cablecast, Access Rights are tied in with the Domain in which they are applied. Check out figure 4.4 on the facing page, which is a screen shot of the Access Rights available in Cablecast. Each Access Right has a parenthetical notation that tells you the Domain(s) that it supports.

There are three types of support:

Location Based : These Access Rights will *ONLY* be used in Roles which have been assigned to a Location Domain.

Location or Channel Based : There are two parts to these Access Rights. First, they will be used in any Roles which have been assigned to a Channel Domain. If they are found in a Role assigned to a Location Domain, then they apply for *ALL* Channels inside the Location.

Global : Roles with any of these Access Rights will grant that ability regardless of the Domain the Role has been assigned for, *and* the Domain the user is currently in. The user will always have the Access Right.

FIGURE 4.3: Three users, with the same responsibilities, for different Domains

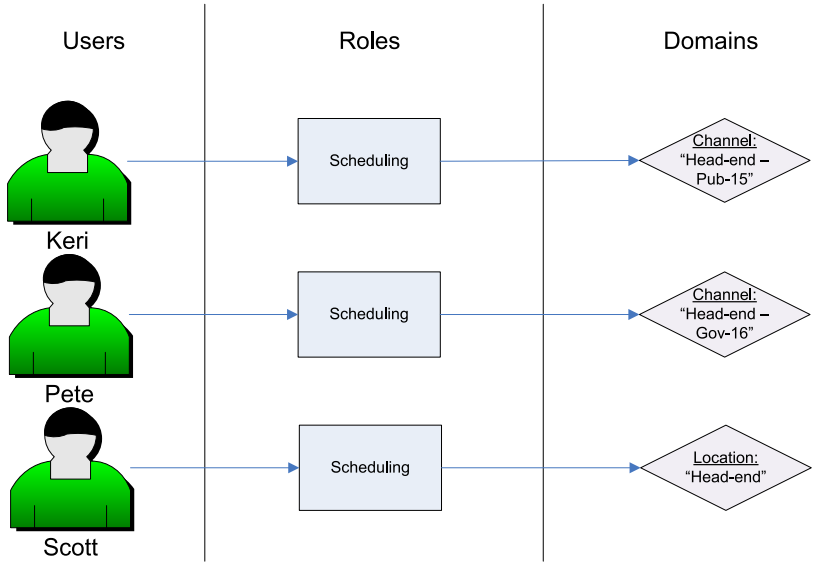
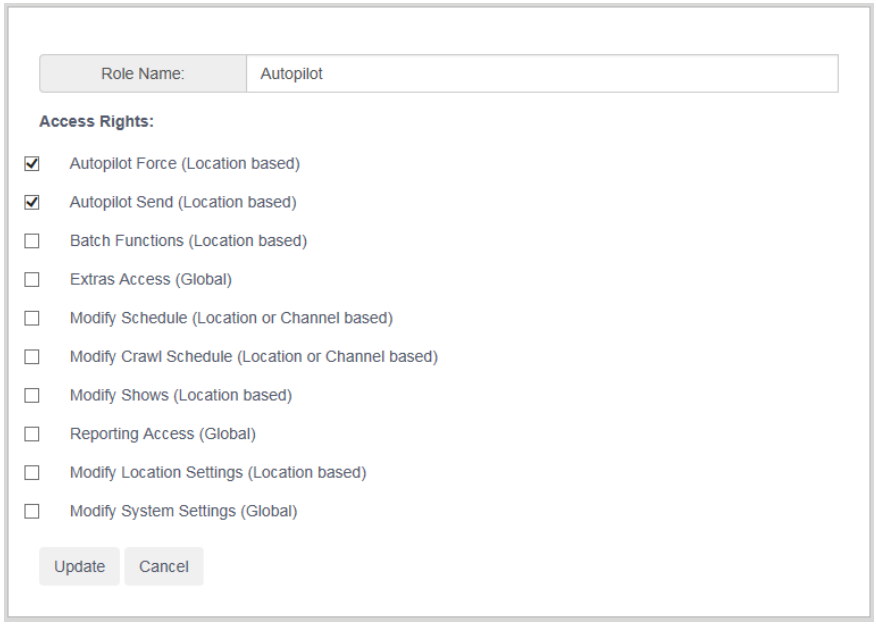


FIGURE 4.4: Access Rights in Cablecast, and their applicable Domains



Examples are definitely in order here. We'll look at each type in turn.

Example: We've set up an "Autopilot" Role at TRMS-TV that includes some Location-based Access Rights. We'd like to give Chad, another dutiful employee, the Autopilot Role. Like any other Role, it needs to be applied for a Domain. If we choose the "Head-end" Location Domain, then Chad is given those Access Rights on the Head-end Location as we expect. If, however, we were to assign the Autopilot Role for a *Channel Domain* (like "Pub-15"), Chad wouldn't be able to use Autopilot at all. As mentioned above, Location-based Access Rights will *ONLY* be used in Roles which have been assigned to a Location Domain. They will be ignored in the context of a Channel Domain.

Example: Earlier, we assigned the "Scheduling" Role to Kari, Pete, and Scott (see figure 4.3 on the previous page). This role contained Access Rights of the "Location or Channel based" type. In Kari and Pete's case, the Scheduling Role is assigned to them for a Channel Domain. This means that both Kari and Pete will be granted these Access Rights for their specific channel, and nowhere else. Scott, on the other hand, was assigned the Role for a Location Domain. In this case, Scott is granted the Access Rights *for every Channel inside the Location*. In other words, Scott can schedule shows on both Pub-15 and Gov-15 with just a single Role assignment.

Example: Finally, there are "Global" Access Rights. In contrast to the Location-based Access Rights that apply only to Location Domains, the Global Access Rights apply everywhere. In other words, having a Global Access Right in any one of your Roles means that you are granted that Access Right everywhere in the software regardless of your current Domain. Let's say that the "Autopilot" Role that we assigned to Chad earlier also has a Global Access Right. As mentioned earlier, if we assigned Chad the Autopilot Role for the Head-end Location Domain, he would be able to do autopilot tasks on the Head-end Location, but not on the Satellite Location. However, since the Global Access Right is also a part of the Autopilot Role, he'll be granted that Global Access Right *everywhere* in the software, including both Head-end *and* Satellite Locations.

4.3 Things to Consider for FrontDoor

4.3.1 FrontDoor Access

Any user account that has been created will, at the minimum, be able to log in to FrontDoor and change his or her password. To allow the user to access other areas in FrontDoor, assign them a FrontDoor Role containing the Access Rights for the appropriate areas. To allow them access to the other applications (Carousel and Cablecast), they must be assigned at least one Role for that application. See section 4.1.1 on page 19 for Carousel details and section 4.2.1 on page 21 for Cablecast details.

4.3.2 Domains: Where'd they go!?

When you start to assign Roles for the FrontDoor application itself, you'll notice that you can't assign them a Domain. What gives?

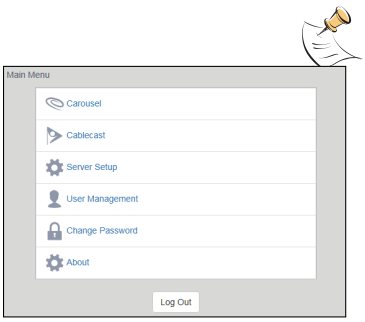
In contrast to Carousel and Cablecast, FrontDoor doesn't have any Domains. More to the point, it has a single Domain: the entire application. Since every Role would be assigned the same domain, we removed the option altogether. All FrontDoor Roles are assigned for the entire FrontDoor application.

5 A Walk-through: Creating Users With a Purpose

We've spent a lot of time talking about the theory of managing users in FrontDoor. In this chapter, the rubber meets the road as we walk through the entire process of creating and maintaining user accounts. We'll use John and Scott (first mentioned in section 3.3 on page 14) as a running example throughout this chapter.

5.1 Step 0: Logging in

Before we can do anything in FrontDoor, we must first log in. In order to access the User Management areas of FrontDoor, be sure to log in with an account that has the proper Access Rights. The Admin account has access to every area of the software, so we'll log in as Admin, as in figure 5.1 on the next page.

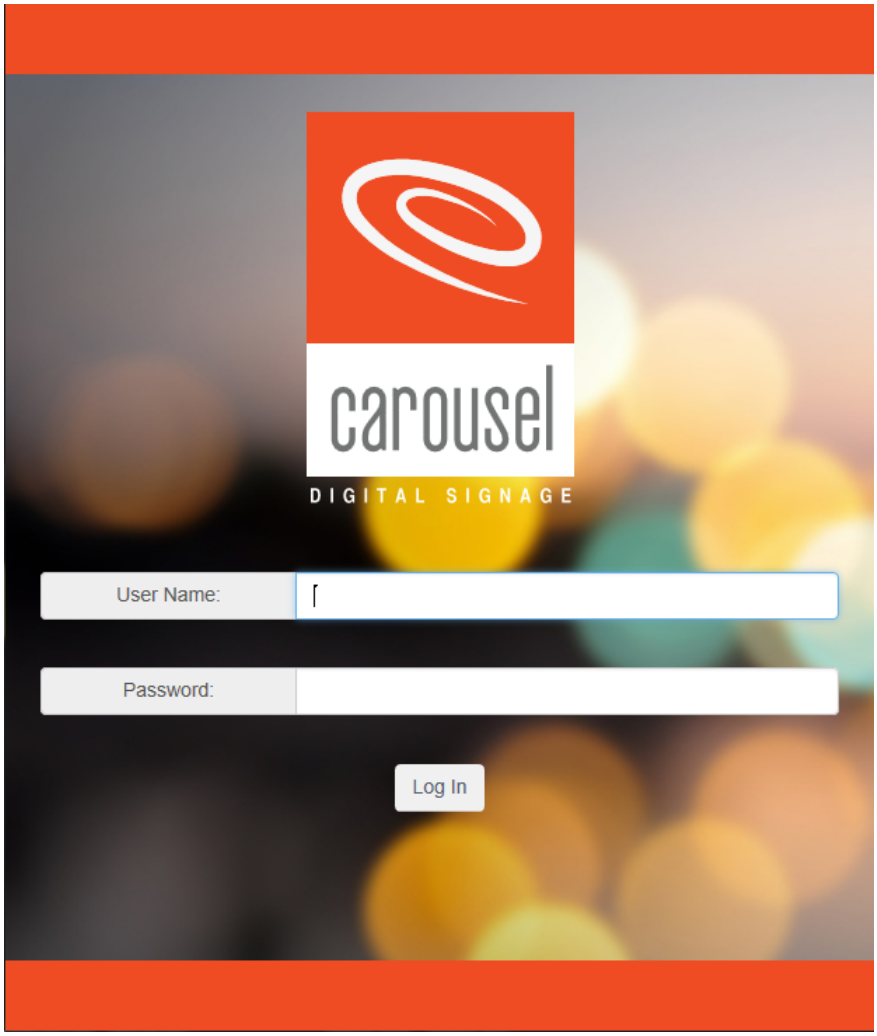


By default, the Admin password is "`trms`".

After successfully logging in, we see the FrontDoor main menu. If you don't see a **User Management** link, then odds are you logged in with an account that doesn't have access to the User Management area of FrontDoor.

Let's proceed. Click on the **User Management** link.

FIGURE 5.1: Logging in as Admin



5.2 Step 1: Create Roles

Once we're in the User Management area, we're presented with several options based on the Tightrope applications you have installed on your system. **User Accounts**, **FrontDoor Roles**, and either **Carousel Roles**, **Cablecast Roles** or both. It's tempting to jump right in and start creating users, however, we're going to take a top-down approach and start with roles. This way, we can think about higher-level "classes" of users first. Later, when we start adding individual users, we've already got an idea about what kind of access is available for them. Click on **Carousel Roles.**

If no Carousel roles have been created on the system, we'll see a screen like the one in figure 5.2 on the facing page.

By default, FrontDoor ships with a few basic Carousel Roles pre-defined. Of course, you can alter them to meet the needs of your installation.

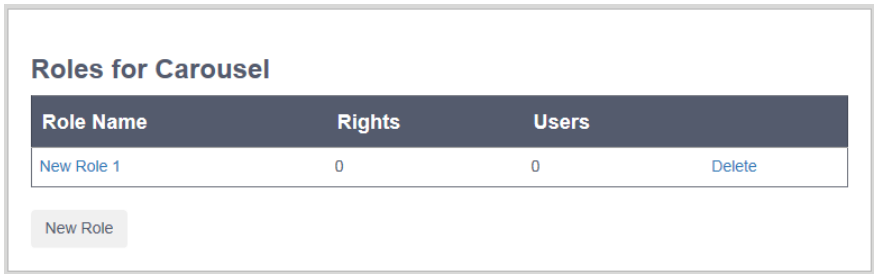
We can't do much without any Roles, so let's create some. Thinking ahead about our intended users John and Scott (Remember them? If not, see section 3.3 on page 14),

FIGURE 5.2: Carousel without any roles.

we know we'd like to have two different Roles. One that allows people to create bulletins, and another that allows users to create bulletins that are automatically approved.

Let's create the first role. Click the **New Role** button. A list of Roles will be created with one new Role, as shown in figure 5.3.

FIGURE 5.3: Carousel with one role.



The list of Roles shows you a couple handy details about each Role. You can see the name of the Role, the number of Access Rights the Role contains, and the number of users who have been given the Role. Since this Role is brand new, it doesn't have any Access Rights or users just yet.

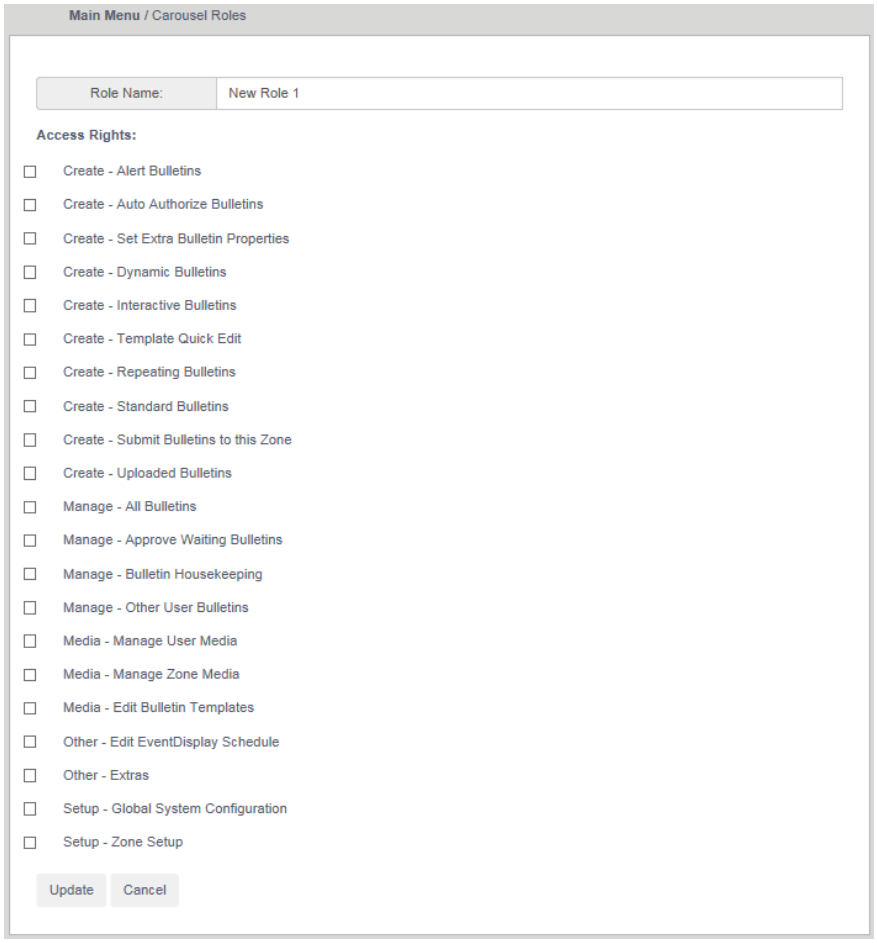
Next, let's customize this new Role so it allows users to create bulletins. Click on the **New Role 1** link. In figure 5.4 on the next page we see the Role Edit screen. There are three parts to this screen. The first allows you to change the Role's name. The second section is a list of which users have been assigned this particular Role. In this case, the Role is brand new and hasn't been assigned to anyone yet, so it doesn't have any users in the list. The third section shows a list of all available Access Rights and lets you pick and choose which Access Rights are granted by this role.

We want this role to allow users to create bulletins, but *not* automatically approve the bulletins. Let's give it a name that describes the role. Enter "`Bulletin Creation`" into the **Role Name** field. Next, assign all of the creation Access Rights by checking the boxes next to their name. Be sure to exclude the **Create - Auto Authorize Bulletins** Access Right, since we don't want automatic approval. When we're done, the screen should look something like figure 5.5 on page 29. Click the **Update** button to save the changes.

We'll be taken back to the Carousel Role List screen. We should see our changes reflected in the list, as in figure 5.6 on page 29. Our role has 9 Access Rights, and it still hasn't been assigned to any users.

Okay, we're halfway done. Next, we want basically the exact same Bulletin Creation role, except this time we want users to have their bulletins to be automatically approved. Go through the same steps to create a new role called "Auto-Authorized

FIGURE 5.4: The Role Edit screen.


Main Menu / Carousel Roles
Role Name:
New Role 1
Access Rights:
Create - Alert Bulletins
Create - Auto Authorize Bulletins
Create - Set Extra Bulletin Properties
Create - Dynamic Bulletins
Create - Interactive Bulletins
Create - Template Quick Edit
Create - Repeating Bulletins
Create - Standard Bulletins
Create - Submit Bulletins to this Zone
Create - Uploaded Bulletins
Manage - All Bulletins
Manage - Approve Waiting Bulletins
Manage - Bulletin Housekeeping
Manage - Other User Bulletins
Media - Manage User Media
Media - Manage Zone Media
Media - Edit Bulletin Templates
Other - Edit EventDisplay Schedule
Other - Extras
Setup - Global System Configuration
Setup - Zone Setup
Update
Cancel

Bulletin Creation." (Make sure to check the **Create - Auto Authorize Bulletins** Access Right for this new role!) When finished, we should have a Role List that looks like figure 5.7 on page 30.

Notice that this new Role has an extra Access Right.

These Roles should cover the access that John and Scott need (for now), so let's move on and create some user accounts.

FIGURE 5.5: Setting up our Bulletin Creation Role.

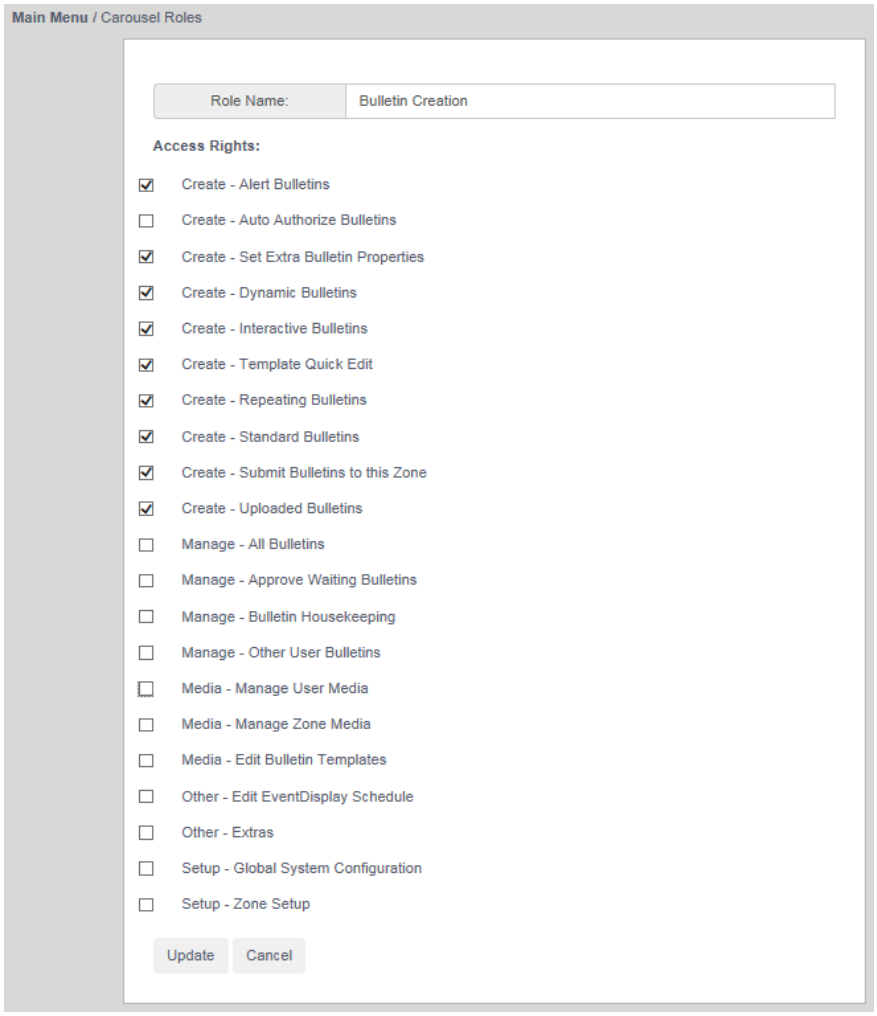

Main Menu / Carousel Roles
Role Name:
Bulletin Creation
Access Rights:
Create - Alert Bulletins
Create - Auto Authorize Bulletins
Create - Set Extra Bulletin Properties
Create - Dynamic Bulletins
Create - Interactive Bulletins
Create - Template Quick Edit
Create - Repeating Bulletins
Create - Standard Bulletins
Create - Submit Bulletins to this Zone
Create - Uploaded Bulletins
Manage - All Bulletins
Manage - Approve Waiting Bulletins
Manage - Bulletin Housekeeping
Manage - Other User Bulletins
Media - Manage User Media
Media - Manage Zone Media
Media - Edit Bulletin Templates
Other - Edit EventDisplay Schedule
Other - Extras
Setup - Global System Configuration
Setup - Zone Setup
Update
Cancel

FIGURE 5.6: The Bulletin Creation Role.

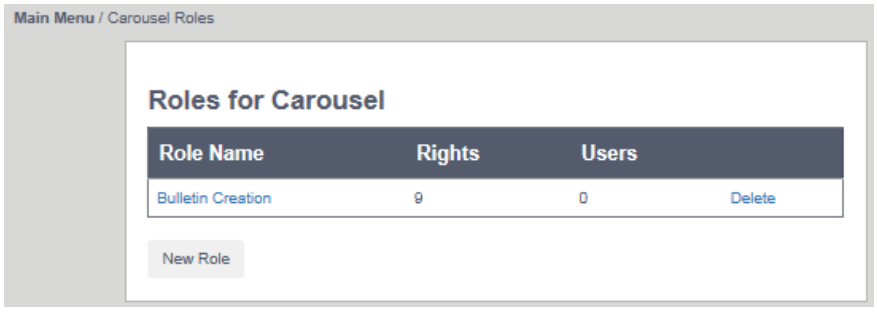
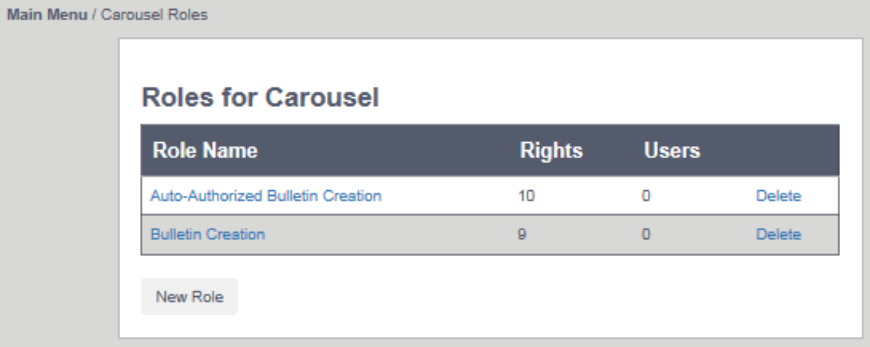


FIGURE 5.7: Both of our Creation Roles.

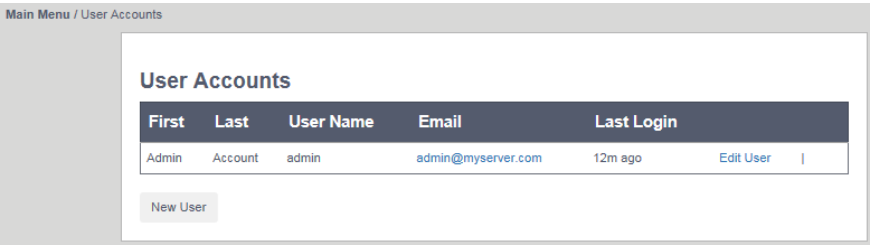


5.3 Step 2: Create Users

Now it's time to give John and Scott an account on the system. We'll start by heading back to the User Management menu. If you're still on the Carousel Roles List screen, click the **Main Menu** link in the header of the page.

Once back at the User Management menu, click on **User Accounts**. We are taken to the User Account List, shown in figure 5.8.

FIGURE 5.8: The default User Account List.



This list will always have at least one user; the Admin account. As mentioned elsewhere, the Admin account is shipped with FrontDoor, has access to all areas of the software, and cannot be deleted[1]. This is most likely the user account that you're currently logged in as, assuming you've been following along with this walk-through.

Since we don't want John or Scott to have full access to the system, let's make a separate account for each of them so they don't have to use the Admin account. To create an account for John, click the **New User** button. We're taken to the New User Account screen, where we can fill out details about John.

In figure 5.9 on the facing page, we've entered John's first and last name, a default password, John's email address, and a few notes[2]. We've also checked the **Send Welcome Message** option. If this option is set, FrontDoor will send a brief message to John's email address, welcoming him to the system and informing him of his new account details. You can see the welcome message in figure 5.10 on the next page.

[1] Another twist: Since Admin always has access to everything in the software, it doesn't really make any sense to assign Admin any Roles. To avoid confusion (and to hammer home the fact that Admin has access to everything), you can't assign any Roles to Admin.

[2] Users will not be able to see the notes on their account, with one exception: If users have access to the User Management area in FrontDoor they will be able to see the notes for all users, including themselves!

FIGURE 5.9: Setting up an account for John.

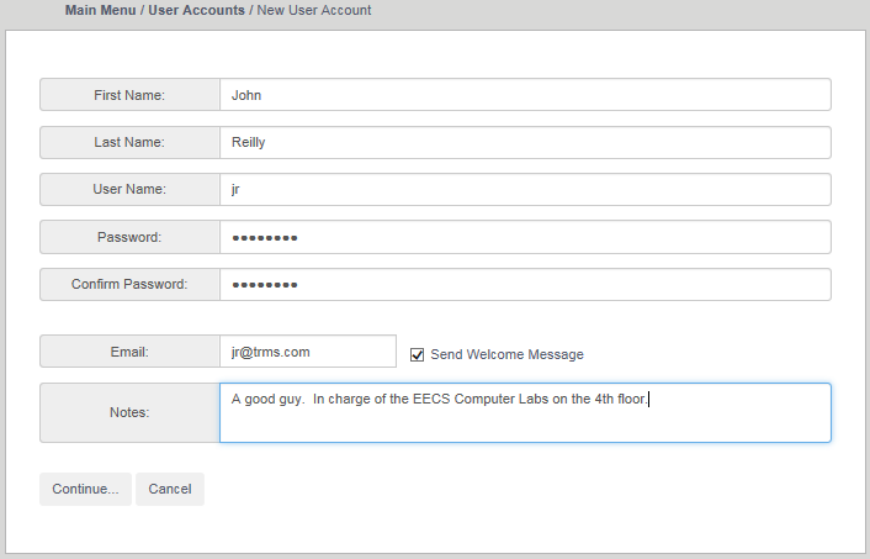
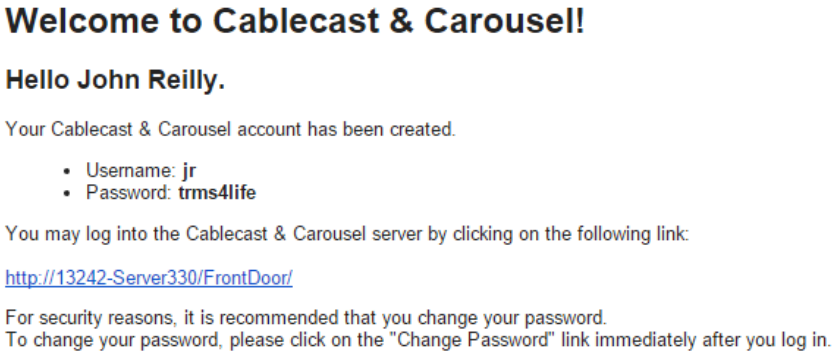


FIGURE 5.10: The welcome email sent to John.



Welcome to Cablecast & Carousel!

Hello John Reilly.

Your Cablecast & Carousel account has been created.

- Username: **jr**
- Password: **trms4life**

You may log into the Cablecast & Carousel server by clicking on the following link:

http://13242-Server330/FrontDoor/

For security reasons, it is recommended that you change your password.
To change your password, please click on the "Change Password" link immediately after you log in.

Before sending any welcome emails to your users, you must first set up a few options elsewhere in FrontDoor. See “Mail Settings” in section 7.4 on page 48, and “Site Login Url” in section 7.2 on page 47.

If you do not customize these settings, the email may not get sent, or might contain incorrect information!

When satisfied, click the **Continue…** button. John’s account will be created, and the welcome message will be sent.

After the account is created, we’re taken to the Role Assignments screen. We’ll tackle this part in section 5.4 on the following page. For now, click on the **Return to User Accounts List** link at the bottom of the screen. Our User Accounts List now includes John’s account, as seen in figure 5.11 on the next page.

We’re still missing Scott. Let’s give him an account, following the same set of steps that we used with John. When finished, we should see three accounts in the list, just like figure 5.12 on the following page.

At this point, both John and Scott have accounts on the system, but they don’t have any Roles. We’ll give them some roles in the next section.

FIGURE 5.11: John's account is now in the list.

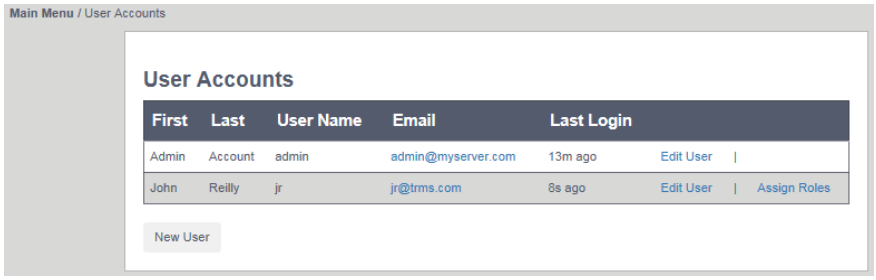
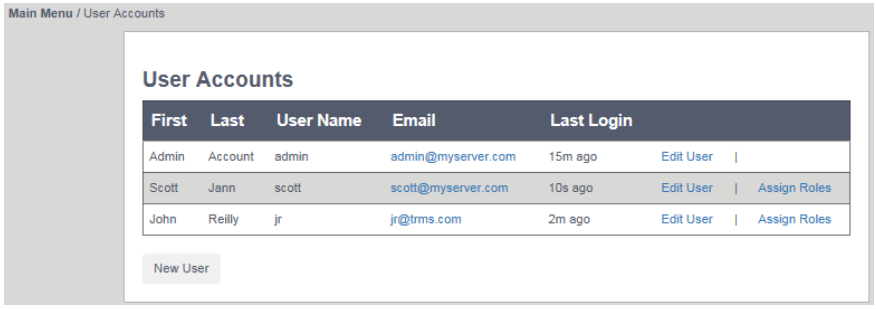

Main Menu / User Accounts
User Accounts
First Last User Name Email Last Login
Admin Account admin admin@myserver.com 13m ago Edit User |
John Reilly jr jr@trms.com 8s ago Edit User | Assign Roles
New User

FIGURE 5.12: John and Scott both have an account.


Main Menu / User Accounts
User Accounts
First Last User Name Email Last Login
Admin Account admin admin@myserver.com 15m ago Edit User |
Scott Jann scott scott@myserver.com 10s ago Edit User | Assign Roles
John Reilly jr jr@trms.com 2m ago Edit User | Assign Roles
New User

5.4 Step 3: Assigning Roles

We have successfully created accounts for our users, but at this point they still can't do very much. Let's give them some Roles. After creating the accounts in the last section, we were automatically taken to the Role Assignments screen. We skipped this step then, but now let's take a closer look. The Role Assignments screen is shown in figure 5.13 on the next page. There are two ways to access this screen. The first we've already seen; after creating a user, you are automatically sent there to set up Roles for your new user. The second way is by clicking on the **Assign Roles** link located on the User Accounts List[3], as seen in figure 5.14 on the facing page.

On the Role Assignments screen, we can see a list of Roles that an individual user has in each application. In figure 5.13, we haven't given John any Roles yet, so each list is empty.

Let's give Scott his Roles. Click on **Assign Roles** for Scott's account. We'll see an empty Role Assignments screen. To assign a Carousel Role, click on the **Assign New Role…** link (figure 5.15 on the next page). A list of drop-down menus will appear as in figure 5.16 on the facing page. These menus allow us to select the Role we'd like to assign, and the Domain to which the role will apply.

For Scott, we'd like to give him the **Auto-Authorized Bulletin Creation** Role that we set up in section 5.2 on page 26. So, we'll select that role in the first drop-down menu (figure 5.17 on page 34).

The second drop-down menu allows you to choose the type of Domain for the Role. In section 4.1.2 on page 19, we described the two types of Domains available to Carousel: Zones and Zone Tags. In Scott's case, we want this Role to apply for all Zones on the West Campus. We can do this by assigning the Role to the West

[3] Note the absence of this link for the Admin account. Once again, you can't give Admin any Roles, because Admin can do everything already!

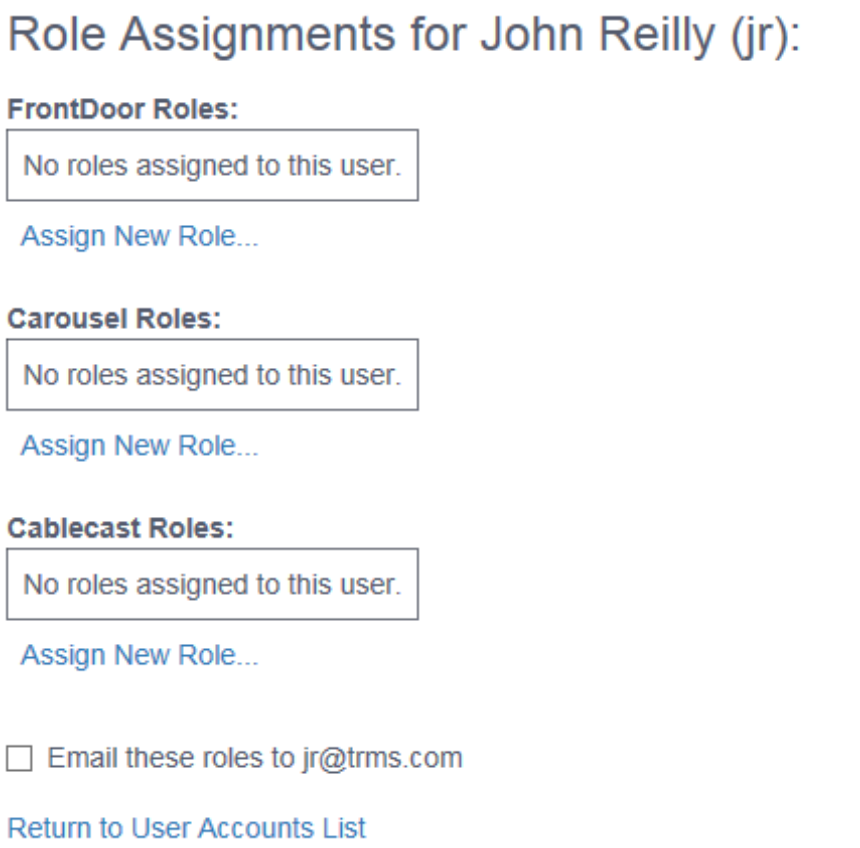

Role Assignments for John Reilly (jr):
FrontDoor Roles:
No roles assigned to this user.
Assign New Role...
Carousel Roles:
No roles assigned to this user.
Assign New Role...
Cablecast Roles:
No roles assigned to this user.
Assign New Role...
Email these roles to jr@trms.com
Return to User Accounts List

FIGURE 5.13: The Role Assignment screen.

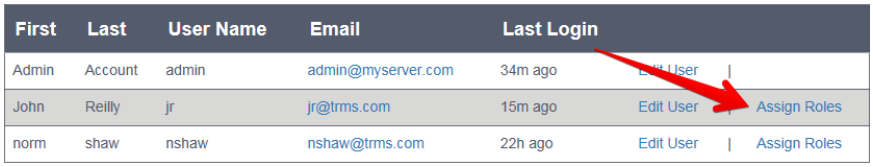


FIGURE 5.14: The Assign Roles link.

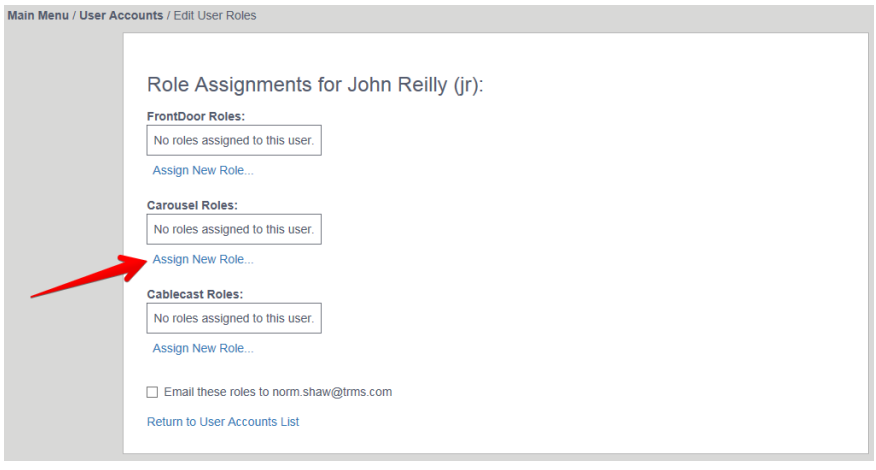

Main Menu / User Accounts / Edit User Roles
Role Assignments for John Reilly (jr):
FrontDoor Roles:
No roles assigned to this user.
Assign New Role...
Carousel Roles:
No roles assigned to this user.
Assign New Role...
Cablecast Roles:
No roles assigned to this user.
Assign New Role...
Email these roles to norm.shaw@trms.com
Return to User Accounts List

FIGURE 5.15: Adding a Role

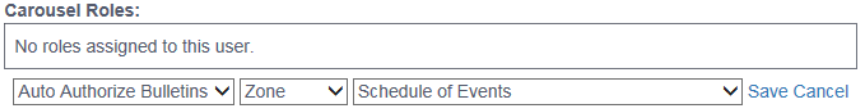
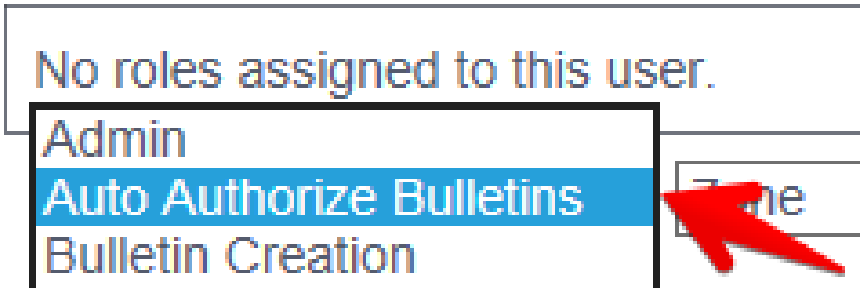


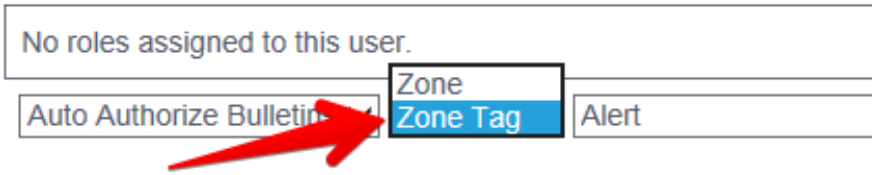
FIGURE 5.16: Menus for adding a new Role.

FIGURE 5.17: Selecting a Role.



Campus Zone Tag. First, select the **Zone Tag** domain type in the second drop down menu (figure 5.18).

FIGURE 5.18: Selecting the Domain type.



By selecting the new Domain type, the third drop-down menu will be updated to list all of the Zone Tags in Carousel. In this list, we can select the **West Campus** tag (figure 5.19).

FIGURE 5.19: Selecting the Domain type.

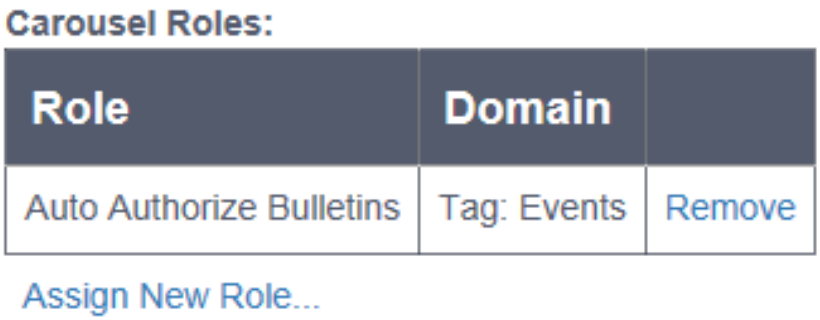
The drop-down menus should look something like figure 5.20. This matches our intentions for Scott's Role, so click the **Save** link. The new Role will be added to the list of Carousel Roles, as in figure 5.21. Success! Scott now has the correct Carousel Role. He will be able to access Carousel and perform the Access Rights included in the Role that we assigned. To get back to the User Accounts List, click the **Return to User Accounts List** link.

FIGURE 5.20: Finished setting up Scott's Role.

Now let's take a look at John. We want him to create bulletins on East Campus Zones, and have automatic approval for any bulletins he makes on the EECS 4th Floor Zone (once again, this scenario is first described in section 4.1.2 on page 19). From the User Accounts List screen, click on **Assign Roles** for John's account.

We create John's first Role in the same way as Scott's. Let's assign him the **Bulletin Creation** Role for the **East Campus** Zone Tag, as in figure 5.22 on the next page. Click **Save** to assign the Role.

FIGURE 5.21: Successfully assigned a Role to Scott.



Next, we need to give him another Role to automatically approve his bulletins for one specific Zone. We'll create an **Auto-Authorized Bulletin Creation** Role for the **EECS 4th Floor** Zone, as in figure 5.23. When finished, John's Carousel Roles should look like figure 5.24 on the next page.

If you would like to inform your users of their Roles, you can check the **Email these roles** option before returning to the User Accounts List. They will be sent an email containing the Roles you've just assigned. Once again, be sure to properly configure both the 'Mail Settings" option (described in section 7.4 on page 48), and the "Site Login Url" option (section 7.2 on page 47).

FIGURE 5.22: Setting up John's first role.

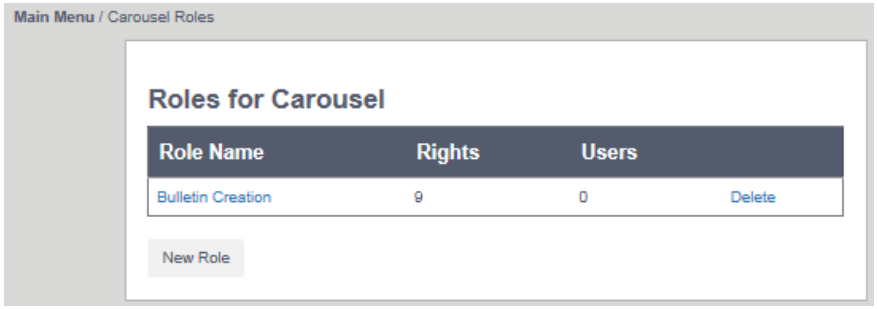
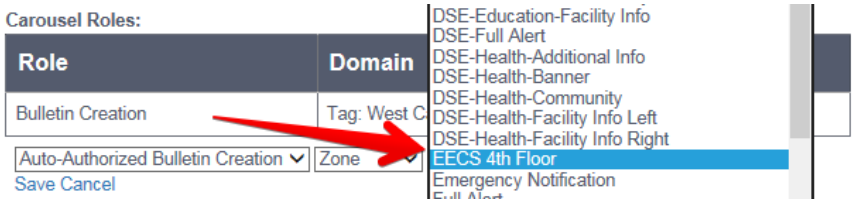
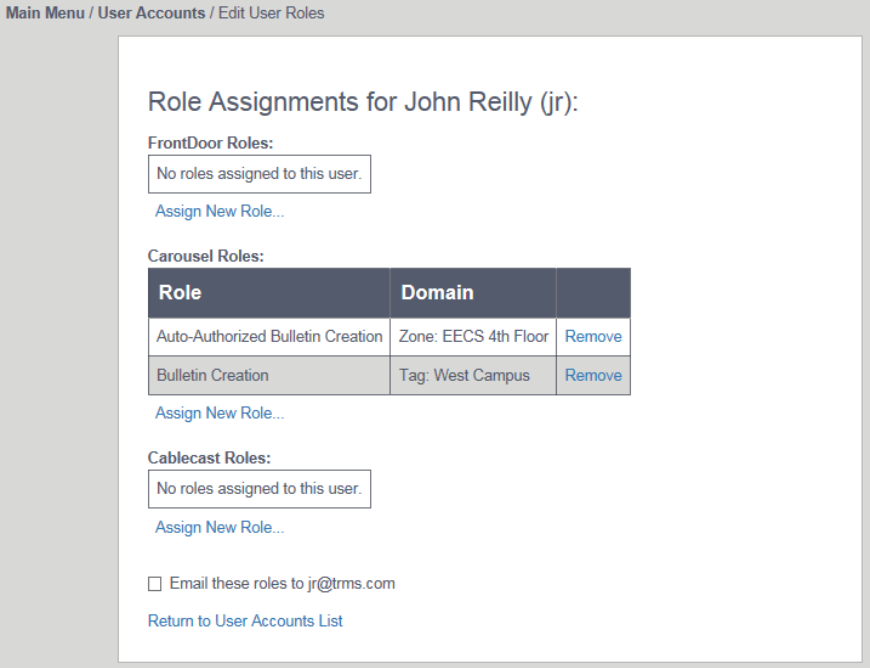


FIGURE 5.23: Setting up John's second role.



At this point, we've created user accounts for both John and Scott, and assigned them the appropriate Roles. Not too bad for a day's work.

FIGURE 5.24: John's final set of Roles.



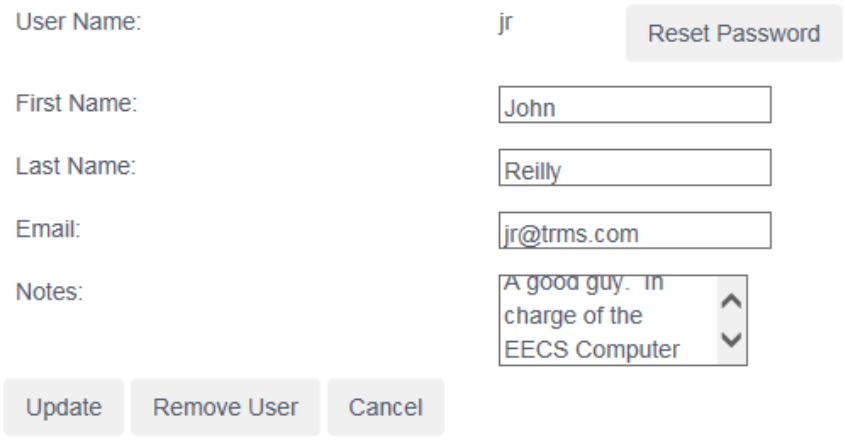
5.5 Day to Day Tasks

Odds are, you'll need to make changes or updates to the User Management area as you start to use the system. This section will cover a few common tasks.

5.5.1 Updating User Information

What happens if one of your users changes his or her email address? Or name? This one is pretty easy. From the User Accounts List (**Main Menu : User Management : User Accounts**), click the **Edit User** link for the user you'd like to update. You'll be presented with the User Edit screen, shown in figure 5.25. On this screen you

FIGURE 5.25: Updating John's user account.



can update a user's name, email address, and any notes you'd like to keep.

5.5.2 Deleting Users

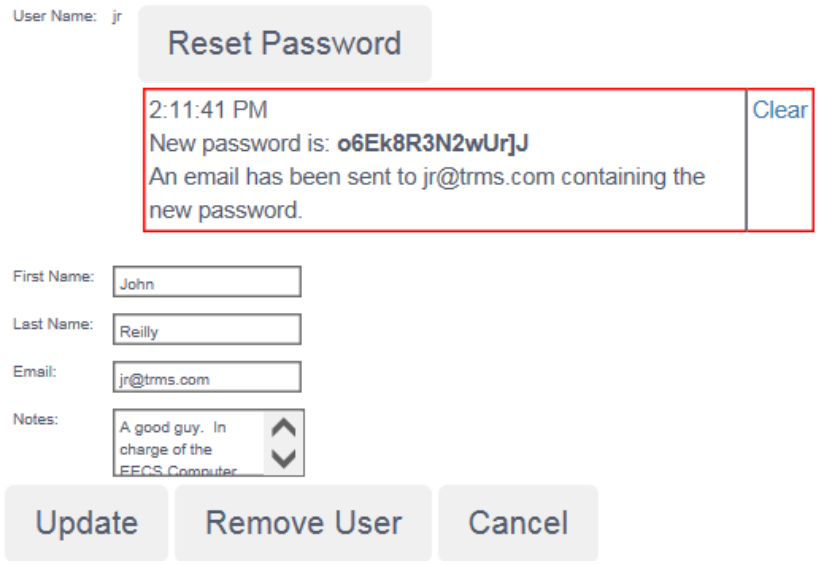
Inevitably, people will come and go in your organization. Rather than keeping user accounts in the system indefinitely, you can remove specific accounts whenever you need to. Looking back on the User Edit screen (shown in figure 5.25 on the preceding page), you can see a button labeled **Remove User**. Clicking on this button will completely remove the user account from the system.

Removing an account will delete all traces of the user from the system. You can't undo this action! (Carousel bulletins created by this user will remain on the system, but will no longer be associated with the account.)

5.5.3 Resetting User Passwords

It's a fact of our technology-laden lives. People will forget their passwords. To generate a new password for a user, click on the **Reset Password** button shown in figure 5.25 on the facing page. A new password will be displayed on the screen (see figure 5.26) and emailed to the user, assuming you have set up your mail servers as described in section 7.4 on page 48.

FIGURE 5.26: The new password will be displayed on the screen.



5.5.4 Unlocking User Accounts

If someone attempts to log in to their account with the wrong password too often over a given period of time, their account will be locked. A locked account will not accept logins (even with the correct password) until the account is unlocked. You can see which accounts are locked at a glance by looking at the User Accounts List. Any locked accounts will be highlighted in red, as seen in figure 5.27 on the next page.

To unlock the account, first click on the **Edit User** link for the afflicted account. The resulting Edit User screen will contain a new button labeled **Unlock User** (see figure 5.28 on the following page). Clicking on this button will unlock the account.

FIGURE 5.27: The new password will be displayed on the screen.

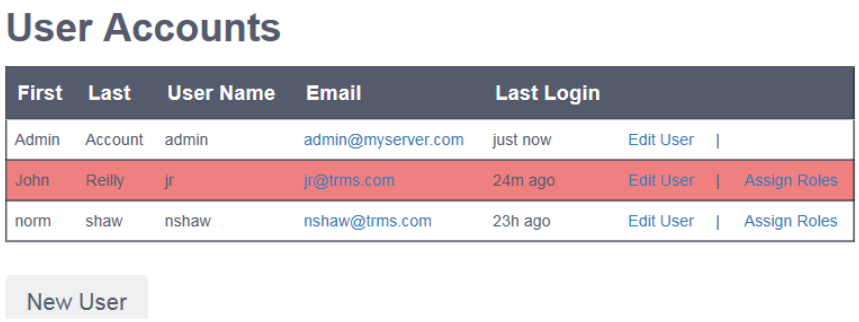
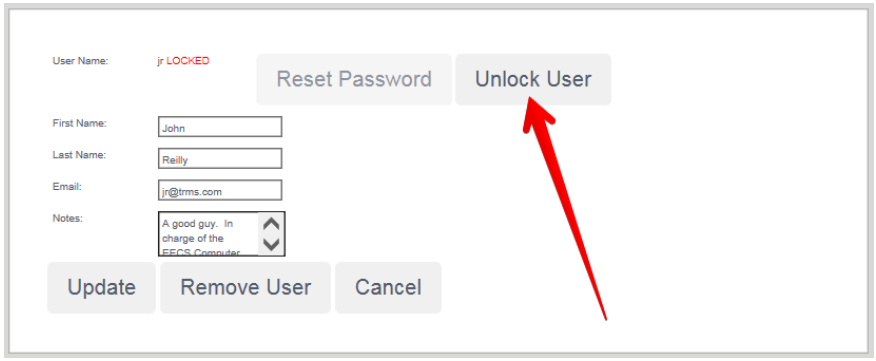


FIGURE 5.28: The User Edit screen for a locked account.



Someone with a locked account probably doesn't remember his or her password. After unlocking the account, it's probably a good idea to reset the password as well.

5.5.5 Changing Passwords

Anyone with a user account in FrontDoor can change his or her password by first logging in with the current password, and clicking on the **Change Password** link on the main menu (figure 5.29 on the next page).

Clicking on the link will take you to the Change Password screen, shown in figure 5.30 on the facing page. Enter the current password, then the desired new password.

New passwords must meet FrontDoor's password strength requirements. To see how to alter the requirements, visit section 7.3 on page 48.

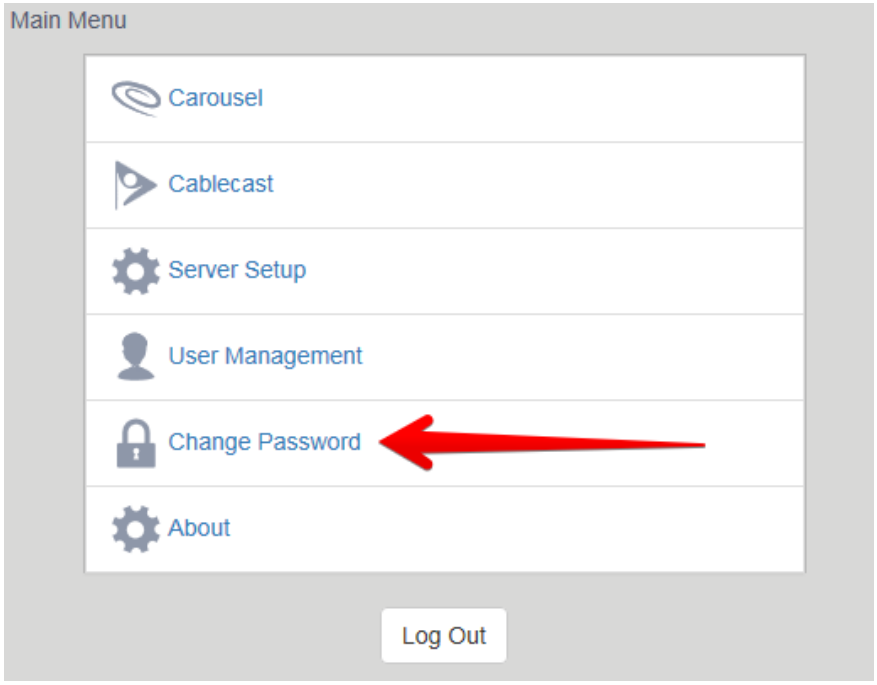


FIGURE 5.29: FrontDoor's main menu contains a link to change the password for your account.

FIGURE 5.30: Changing your password.

II. Server Setup

6 Introduction to Setting Up Your Server

The Server Setup area of FrontDoor is where you will be configuring options for the entire server. In this chapter, we will take a brief look at what options are available, and how the affect the system.

By default, your FrontDoor server ships with default values that must be changed before you can use your system effectively. See section 6.2 on page 46 for details on which settings require your attention.

6.1 An Overview of Server Setup

After clicking on **Server Setup** from FrontDoor's main menu, you will see FrontDoor's Server Setup menu (shown in figure 6.1 on the next page). Each section of the menu is described below.

6.1.1 Site Name

The Site Name refers to the text that is displayed in the header of the Tightrope Web Interface. This header is shown on all web applications that are run on this FrontDoor server. Generally, the Site Name is set to the name of your organization.

See section 7.1 on page 47 for details.

6.1.2 Site Login Url

Some parts of FrontDoor are designed to generate a hyperlink that will take users to the FrontDoor login page. For example, the new user welcome email (see section 5.3 on page 30) contains this hyperlink so your users know where to login so they can start using the system.

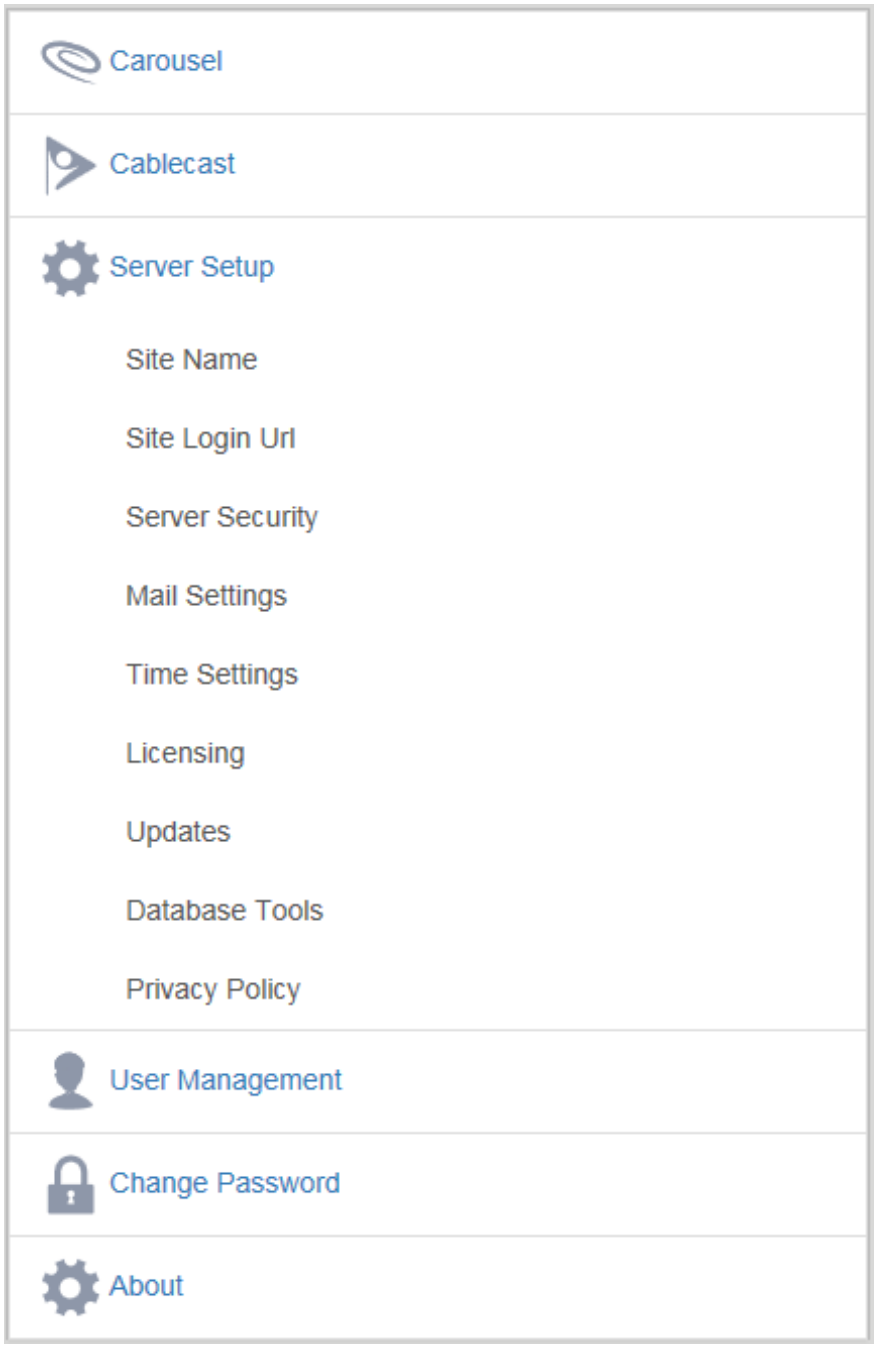
See section 7.2 on page 47 for details.

6.1.3 Server Security

This section allows you to alter basic security measures of your server. You can control how strong user passwords need to be, the length of time before users are automatically logged out due to inactivity, and choose whether or not visitors are automatically taken to the FrontDoor login screen.

See section 7.3 on page 48 for details.

FIGURE 6.1: FrontDoor Server Setup Menu



6.1.4 Mail Settings

! → FrontDoor relies heavily on sending email to the users of the system. An email is sent to users when their account is created (see section 5.3 on page 30), when you assign them Roles (section 5.2 on page 26), and when you reset their passwords (section 5.5.3 on page 37). In this section you can configure the email server that FrontDoor will use.

See section 7.4 on page 48 for details.

6.1.5 Time Settings

! → If your system contains multiple Tightrope servers, it is imperative that their system clocks are kept in sync. The servers will sync their clocks to the system clock on the FrontDoor server. This section allows you configure the FrontDoor server to sync its own time to an external source.

See section 7.5 on page 50 for details.

6.1.6 Licensing

Software from Tightrope Media Systems must be properly licensed before it can be used. In the Licensing section, you can enter a license code for the software that you have purchased. The software is usually pre-licensed on the server before it is shipped, so you should only need to enter this section if you have purchased additional software or upgrades.

See section 7.6 on page 52 for details.

6.1.7 Updates

New versions of Tightrope software can be downloaded from the Updates section. You will be required to enter an update key before gaining access to the software updates. To obtain an update key, contact Tightrope Media Systems Technical Support. Contact information can be found in section 1.2 on page 7.

See section 7.7 on page 55 for details.

6.1.8 Database Tools

Your system makes extensive use of databases for storing and retrieving important data. It is a good idea to regularly backup these databases to protect from losing your data in the event of a disaster. In the Database Tools section, you can backup any or all of your databases to a variety of locations.

See section 7.8 on page 56 for details.

6.1.9 Privacy Policy

If there are any errors that occur in our software, we want to know about it. Tightrope software has a mechanism for automatically sending the details of an error to us so we can fix it in a future release. In this section, you can control whether or not this information is sent to us.

See section 7.9 on page 58 for details.

6.1.10 About

This screen will tell you what version of the FrontDoor software your system is running. If you encounter a problem, our Technical Support team will want to know the version number of your software so they can accurately track issues.

See section 7.10 on page 58 for details.

6.2 Important Things to Set Up

Some areas of Server Setup are more critical to the proper usage of your system than others. At the minimum, you will want to visit the following sections when initially setting up your server.

Site Login Url : details on section 7.2 on the next page

Server Security : details on section 7.3 on page 48

Mail Settings : details on section 7.4 on page 48

Time Settings : details on section 7.5 on page 50

7 Server Setup Reference

This chapter describes FrontDoor's Server Setup options in detail.

7.1 Site Name

The Site Name section (see figure 7.1) sets the name of the server, as seen in web page headers.

Site Name : The name of your server or organization.
Example: Tightrope Media Systems

FIGURE 7.1: Main Menu : Server Setup : Site Name

7.2 Site Login Url

These settings should be properly configured before deploying your FrontDoor server.

This Url is used to direct users to the FrontDoor login page from external sources, such as an email. (see figure 7.2)

Site Url : The Url to the FrontDoor login page.
Example: http://<yourserver>/FrontDoor/Login.aspx

FIGURE 7.2: Main Menu : Server Setup : Site Login Url

7.3 Server Security

These settings should be properly configured before deploying your FrontDoor server.

The Server Security section allows configuration of various security options. (see figure 7.3)

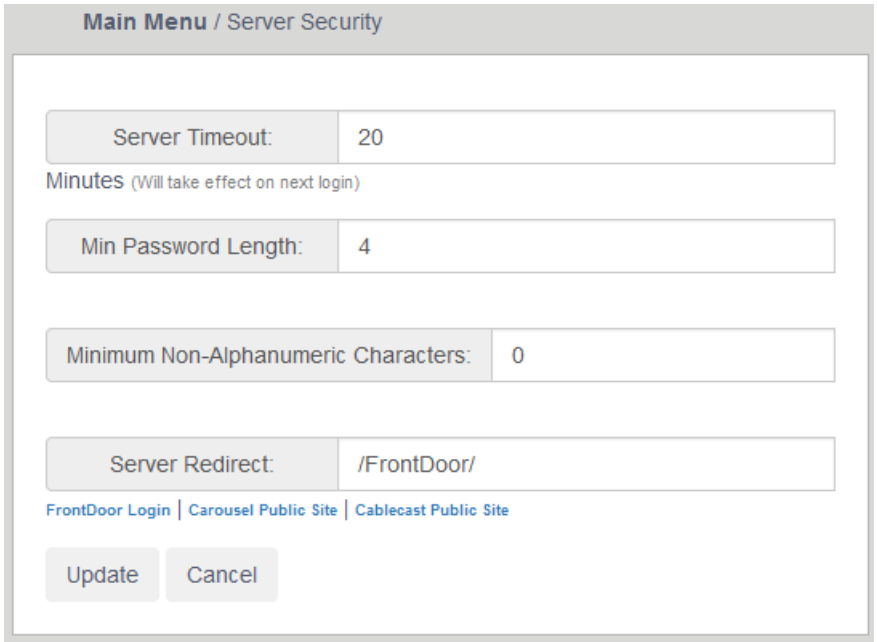
Server Timeout : Number of minutes before inactive users are automatically logged out of the system.
Example: 20 (minutes)

Minimum Password Length : Forces all user passwords to be at least this many characters in length.
Example: 4 (all passwords must be greater than or equal to four characters in length)

Minimum Non-Alphanumeric Characters : Forces all user passwords to have at least this many "special" characters (characters that are not letters or numbers, e.g., '!', '@', '#', '$', '%', '&', '*', etc.).
Example: 0 (passwords don't need special characters)
Example: 5 (passwords need at least five special characters)

Server Redirect : Http requests for the server's root directory will be redirected to this site. Useful if you want visitors to be automatically taken to a public-friendly site.
Example: /FrontDoor/ (users will be redirect to the FrontDoor login page)
Example: /Carousel/Public/ (users will be redirect to Carousel's public site)

FIGURE 7.3: Main Menu : Server Setup : Server Security



7.4 Mail Settings

These settings should be properly configured before deploying your FrontDoor server.

If your organization doesn't have an email server that you can use, there are other options available. See section D.6 on page 74

FrontDoor uses the settings in the Mail Settings screen to connect to an email server and send emails to users. Several Tightrope applications depend on the ability to send email (see figure 7.4).

Smtp Mail Server : The address of the Simple Mail Transport Protocol email server that FrontDoor can connect to.
Example: mail.myserver.com

Port : The port on the email server that is listening for requests
Example: 25 (25 is the default port, but your organization might require a different port).

Use Authentication : If your email server uses authenticated Smtp, check this box.

Enable SSL : If your email server requires a Secure Socket Layer connection, check this box.

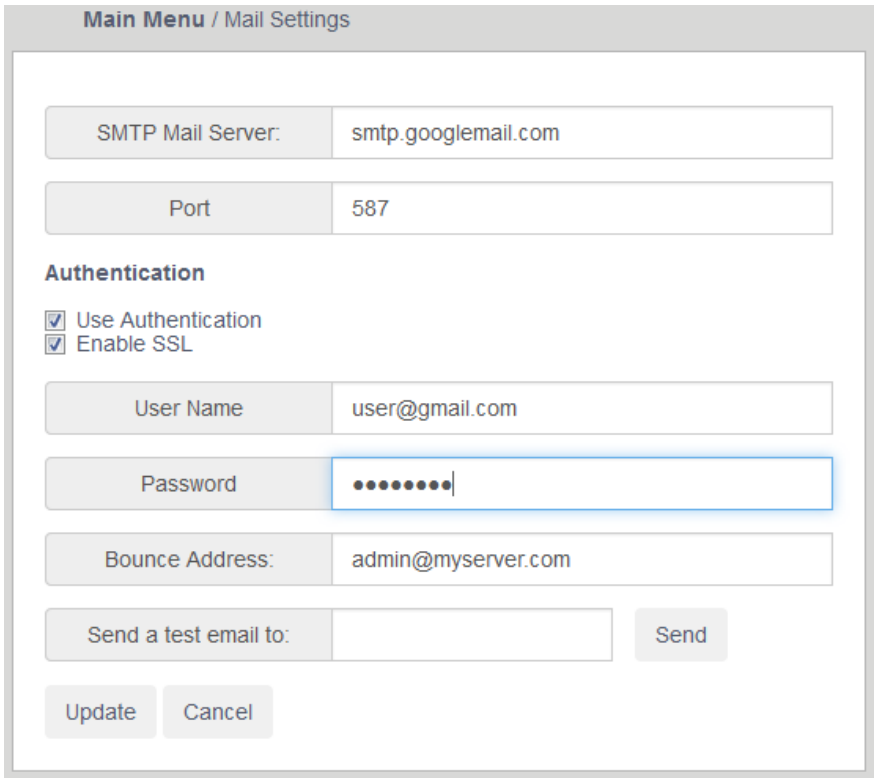
Username : If you have the "Use Authentication" box checked, enter the username required to log into the Smtp server.

Password : If you have the "Use Authentication" box checked, enter the password required to log into the Smtp server.

Bounce Address : This is the "From" address used by all email sent from FrontDoor (and other applications).
Example: admin@myserver.com (Usually the person in charge of maintaining the FrontDoor server

Send a test email to : By clicking on "Send," a test message will be sent to this address. Useful to test the mail settings that you have configured.

FIGURE 7.4: Main Menu : Server Setup : Mail Settings



7.5 Time Settings

These settings should be properly configured before deploying your FrontDoor server.

Your Tightrope server needs to have its system clock updated regularly. FrontDoor gives you four different ways of keeping the clock in sync:

Tightrope : See section 7.5.1.

Windows : See section 7.5.2.

Domain Controller : See section 7.5.3 on the facing page.

None : See section 7.5.4 on page 52.

On the Time Settings screen, (**Main Menu : Server Setup : Time Settings**) the "Sync Settings" drop down menu lets you select which style of time synchronization to use, and will reveal other options for the selected synchronization method.

7.5.1 Tightrope Time Synchronization

The Tightrope Time Synchronization method allows you to select which NTP[1] server to use, and how often to update. It is the most flexible time synchronization method.

NTP uses UDP port 123 to communicate. Be sure to set your firewall to allow traffic on this port.

For a list of publicly available NTP servers, see section D.5 on page 73.

Service Status : Indicates whether or not the time synching service is running.

Time Server : The NTP server that your system's clock will synchronize to.
Example: time.trms.com

Update Interval : Determines how frequently (in seconds) the clock will synchronize.
Example: 600 (equates to 10 minutes)

Recent Activity : Displays when the last update occurred, how much correction took place, when the next update will occur, and keeps a history of previous updates.

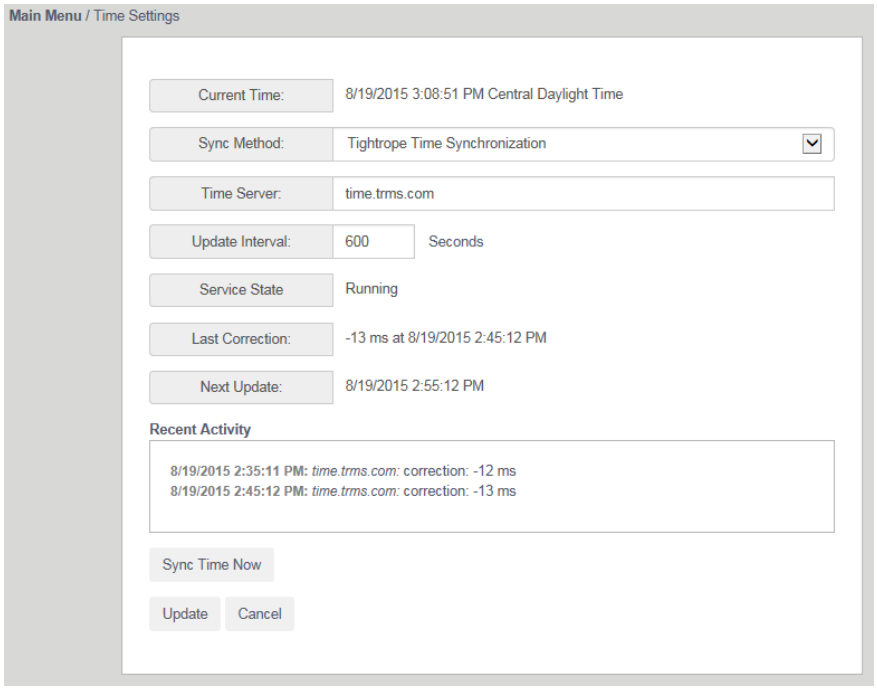
7.5.2 Windows Time Synchronization

The Windows Time Synchronization option uses the same time synchronization subsystem that Windows itself uses. It is a bit more restrictive than Tightrope Time Synchronization in that it doesn't allow you to adjust how often synchronization occurs. Windows uses a slightly different version of NTP called SNTP[2], which may restrict which time servers that you can connect to.

SNTP uses UDP port 123 to communicate. Be sure to set your firewall to allow traffic on this port.

[1] NTP stands for "Network Time Protocol" and is widely used on the internet. See http://www.ntp.org/ or http://en.wikipedia.org/wiki/Network_Time_Protocol for more information.
[2] See http://www.ntp.org/ntpfaq/NTP-s-def.htm#AEN1253 for details on SNTP.

FIGURE 7.5: Main Menu : Server Setup : Time Settings Using Tightrope Time Synchronization



For a list of publicly available NTP servers, see section D.5 on page 73.

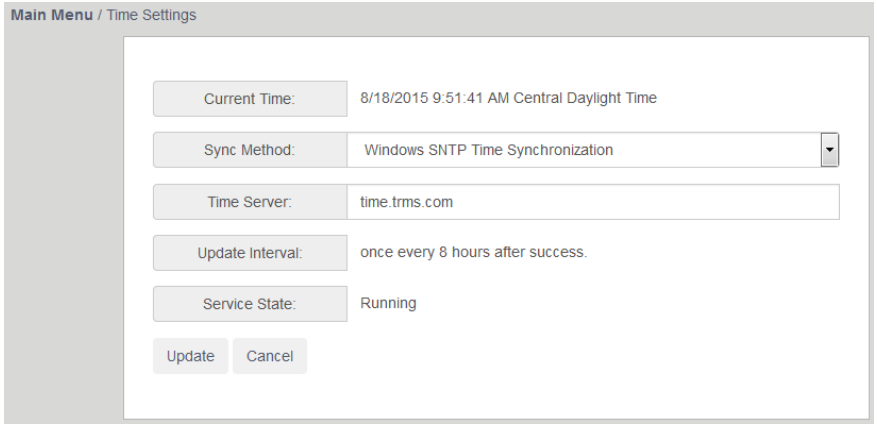
Service Status : Indicates whether or not the Windows time synching service is running.

Time Server : The NTP server that your system's clock will synchronize to.
Example: time.trms.com

Update Interval : Displays how often Windows will synchronize the clock to the Time Server.

Recent Activity : Displays a brief status report of the Windows Time Synchronization service.

FIGURE 7.6: Main Menu : Server Setup : Time Settings Using Windows SNTP Time Synchronization



7.5.3 Domain Controller Time Synchronization

Your organization might have a Windows Domain Controller managing all computers on your network. If the FrontDoor server is joined to a domain, the "Domain

Controller Time Synchronization" option will appear. If you select this method, the FrontDoor server's clock will be automatically synched to the Domain Controller.

Service Status : Indicates whether or not the Windows Domain time synching service is running.

Time Server : The Domain Controller that your system's clock will synchronize to.

Update Interval : Displays how often Windows will synchronize the clock to the Domain Controller.

Recent Activity : Displays a brief status report of the Windows Domain Controller Time Synchronization service.

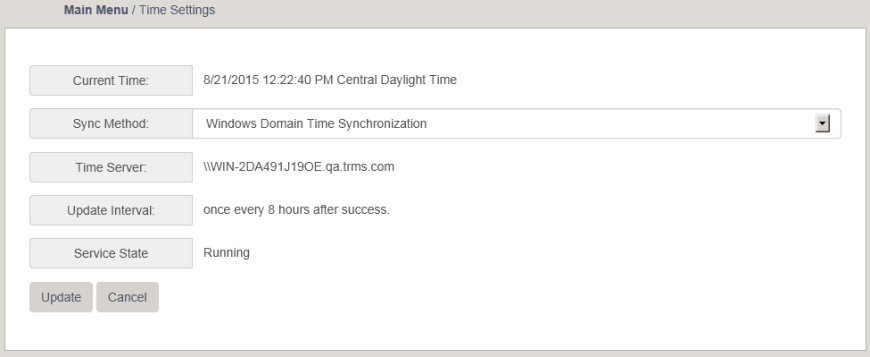


FIGURE 7.7: Main Menu : Server Setup : Time Settings Using a Domain Controller for Time Synchronization

7.5.4 No Time Synchronization

You may choose to run your own time synchronization software. In this case, be sure to disable FrontDoor's time synchronization by selecting "No Time Synchronization." This will prevent any conflicts between the software.

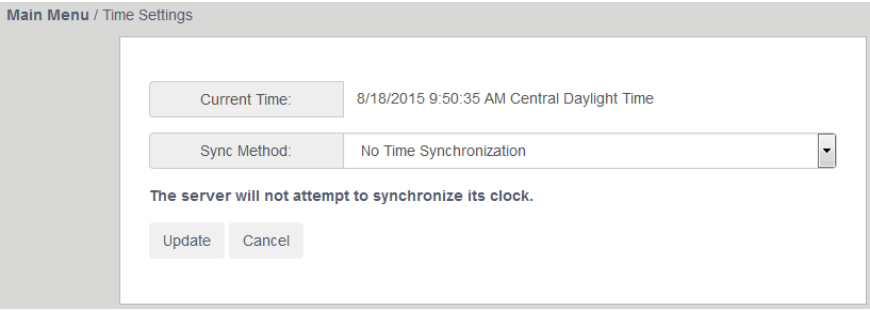


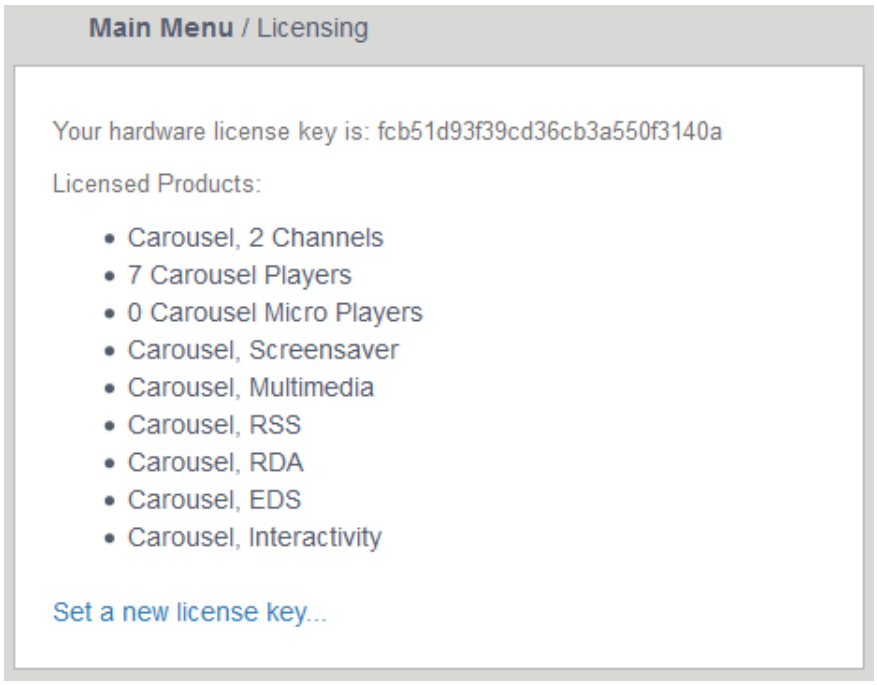
FIGURE 7.8: Main Menu : Server Setup : Time Settings Turning off any time synchronization

7.6 Licensing

The Licensing section of FrontDoor's Server Setup allows to you see what Tightrope products you have purchased and are active on your system. If you ever wish to upgrade your system (by adding a new Channel License to Carousel, for example), you will most likely need to enter a new "license key," which is a long string of letters and numbers. Additionally, each system that ships from Tightrope Media Systems has a unique Hardware ID that is used to validate license keys. In other words, any given license key will only be valid on the system that it was generated for.

The main licensing screen looks like figure 7.9. On this screen you can see the list of products you have purchased. On this screen you will also find your unique Hardware ID, which you may need to provide in order to obtain new license keys.

FIGURE 7.9: Main Menu : Server Setup : Licensing

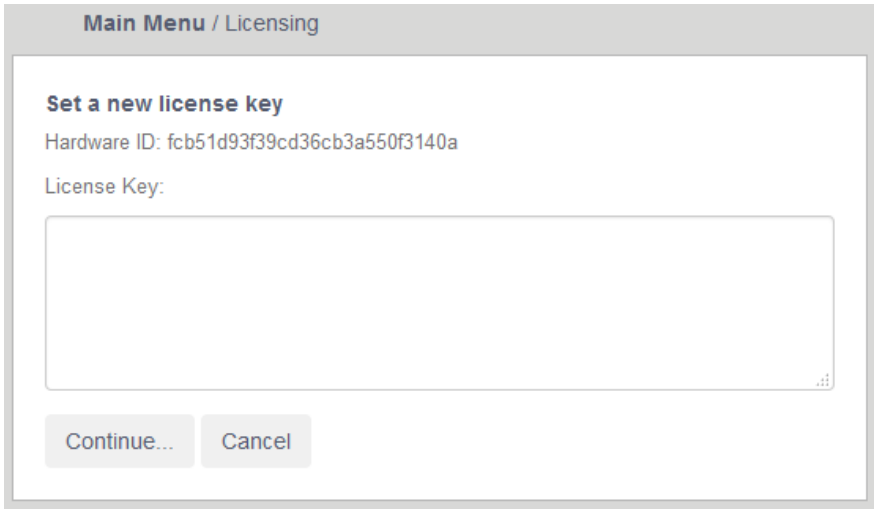


7.6.1 Setting a New License Key

Once you have obtained a new license key from Tightrope Media Systems, click on the **Set a new License Key...** link. You will be taken to a screen like the one shown in figure 7.10. Copy and paste your new license key *exactly* as it comes from Tightrope Media Systems into the **License Key** field, and then click **Continue**.

License keys do not contain spaces.

FIGURE 7.10: Main Menu : Server Setup : Licensing Installing a new License Key



7.6.2 Confirming a New License Key

After you have entered the new license key, you will be taken to a confirmation screen like the one in figure 7.11. On the left side of the screen you will see the list of products that your new license key is good for. On the right side of the screen in smaller text you will see the list of products that you are *currently* licensed for.

! → The distinction between these lists is important because the list on the left will be *replacing* the list on the right. Be sure to double check that the new list of products includes your upgrade *plus all of your existing products*.

When you are satisfied, click the **Set New License** button to commit the new license key to the system.

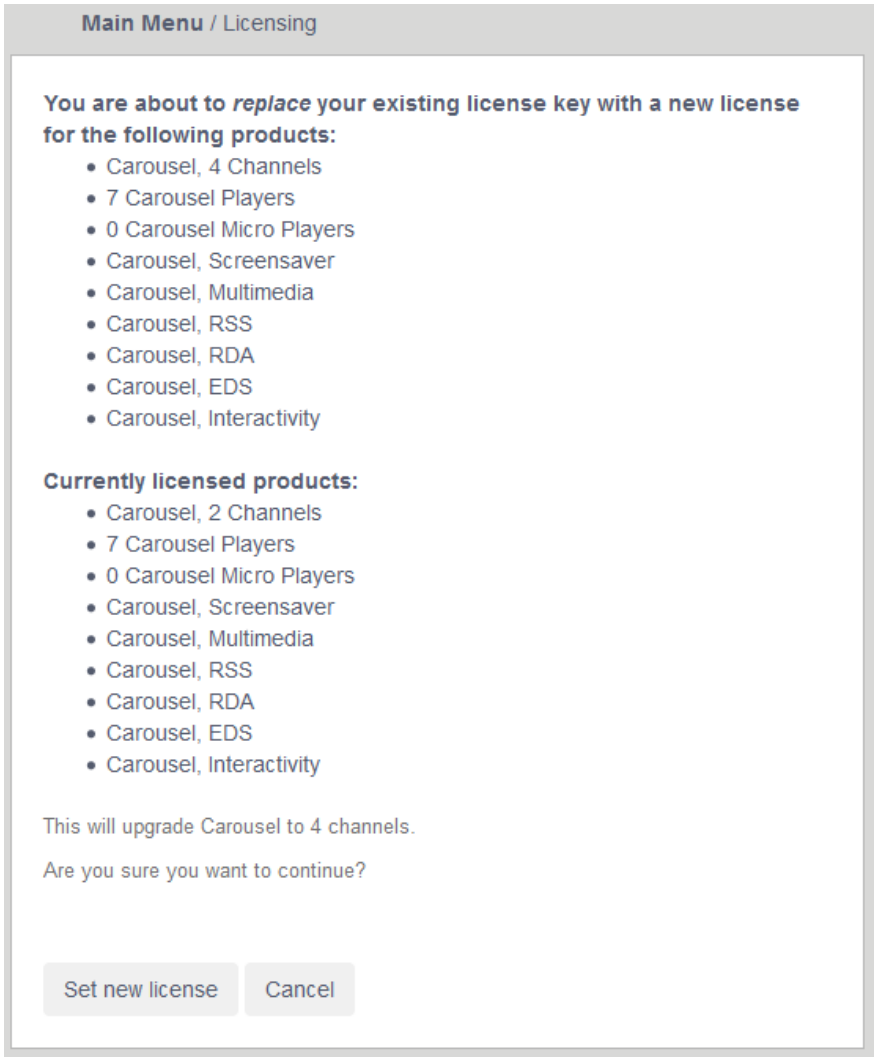


FIGURE 7.11: Main Menu : Server Setup : Licensing Confirming a new License Key

7.7 Updates

To obtain updates to your Tightrope Media Systems software, you will need to acquire a "Download Key" which gives you access to our updates server for a limited time. To obtain the download key, contact Tightrope Media Systems Technical Support (see section 1.2 on page 7). After you have received your download key, you may enter it on the **Main Menu : Server Setup : Updates** screen shown on figure 7.12.

FIGURE 7.12: Main Menu : Server Setup : Updates

Accessing the updates server requires that your FrontDoor server be connected to the internet. If your FrontDoor server does not have internet access, you can visit the updates site from a different computer by browsing to http://updates.trms.com/.

Your download key is only valid for a limited amount of time, usually about 10 days from the time it is issued to you.

7.7.1 Selecting Updates for Download

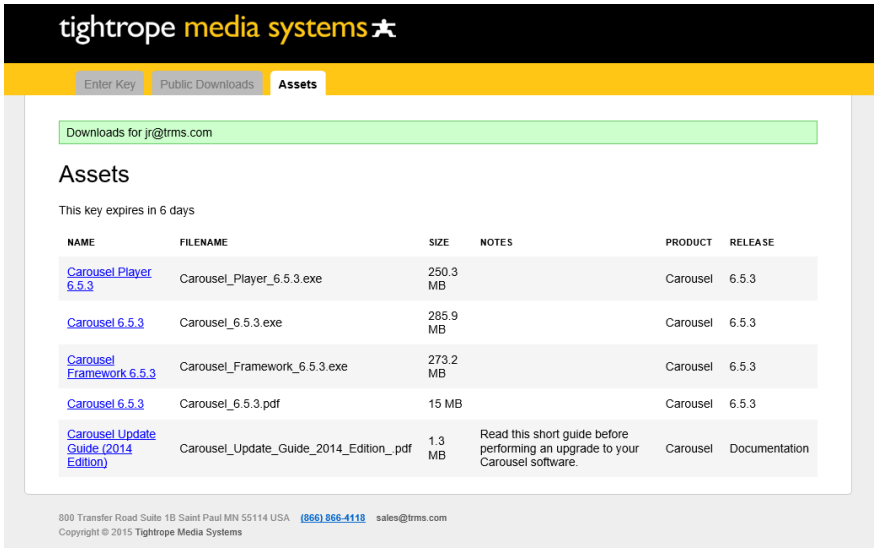
After entering a valid download key, you will be presented with a list of files to download, similar to figure 7.13 on the next page. Please read the "Notes" column for each download, as it may contain critical information about that particular file. Often, a "Readme" file will be included with your download list. Before installing any updates, *make sure to download and read the "Readme" file!*

Always read the "Readme" files!

Although we try to make the update process as simple as possible, occasionally there are steps that must be completed in a specific order for the update to be successful. These steps will be outlined in the Readme file.

Each file in the list may be downloaded a limited number of times. We recommend downloading all available updates once to a single computer, and then distributing them via your own network rather than downloading them multiple times from the updates site.

FIGURE 7.13: Main Menu : Server Setup : Updates List of available updates



7.8 Database Tools

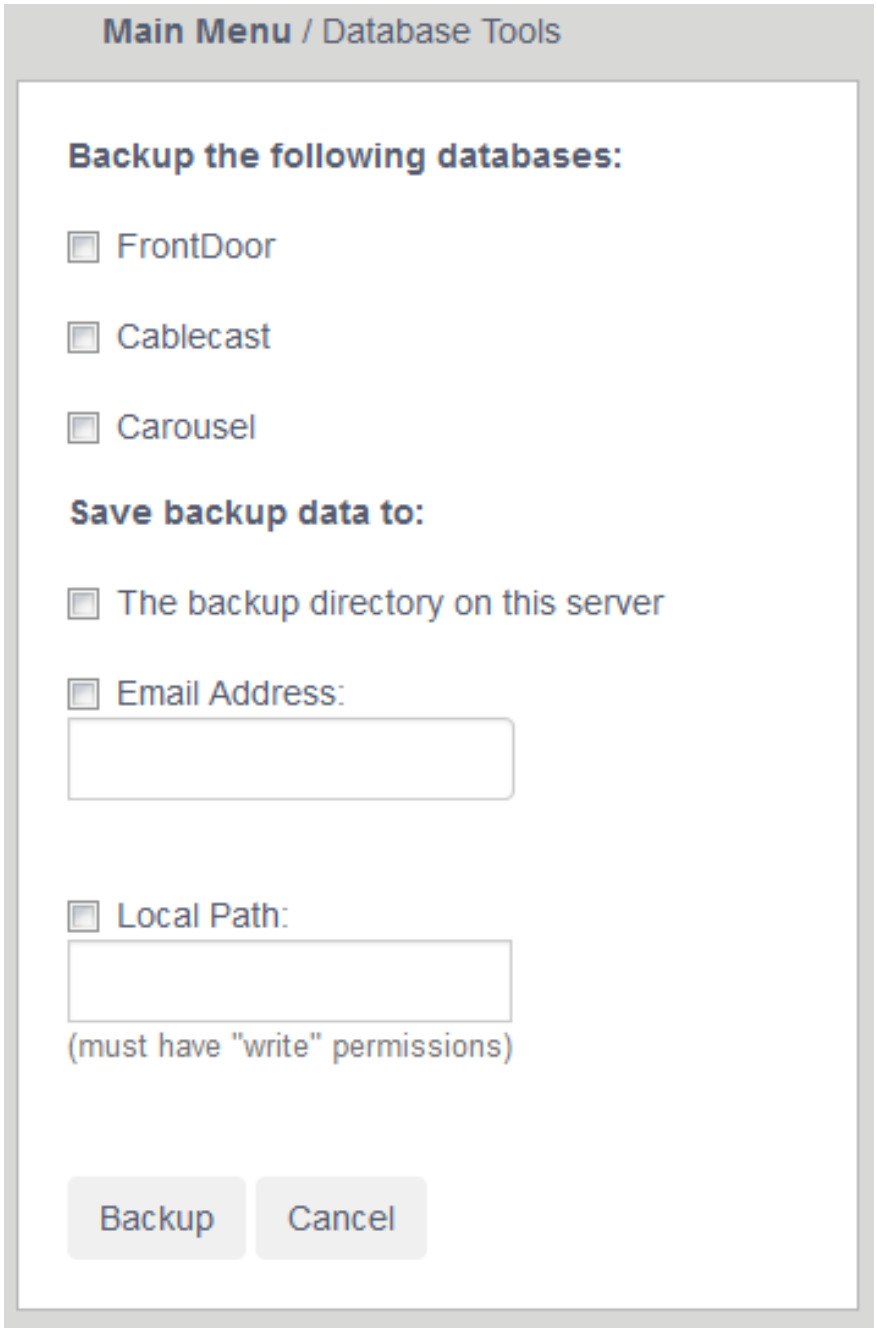
The Database Tools screen allows you to backup your data. As in figure 7.14 on the facing page, you will see each of the databases that are installed on your system, and you will be given a choice of backup locations. You can choose any combination of databases and backup locations.

Backup Directory : Databases will be saved to a directory on the FrontDoor server. This directory is specified in the "BackupDirectory" variable in the "web.config" file located on your FrontDoor webserver.

Email Address : Databases will be emailed as an attachment to this email address.

Local Path : Databases will be saved to this directory on your FrontDoor server. The FrontDoor webserver user account must have write access to the directory.

FIGURE 7.14: Main Menu : Server Setup : Database Tools



7.9 Privacy Policy

Tightrope Media Systems is dedicated to finding and fixing any errors that may occur in our software packages. In order to help us fix errors, we like to collect information about how and where the error occurred. This information can be extremely helpful when tracking down the cause of an error, however, *some of this information might contain personally identifiable data.* This screen will allow you to control what data we may collect, or, you can choose to not participate in our data collection at all.

We will **never** divulge collected data to any third-party unless required to do so by law.

Do not collect any data : When an error occurs, we will not collect any data about it at all.

Collect basic error data : This will allow us to collect data about where the error occurred. The only information we will receive will be the name of the error, and where in our code it occurred. We will not be able to trace any of this data back to you.

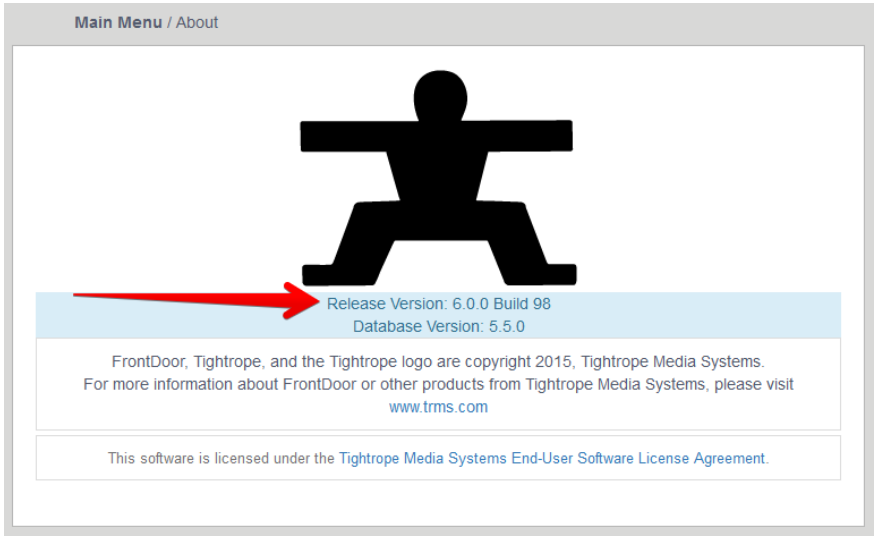
Collect error context data : In addition to basic error data, this will allow us to collect data about what was going on when the error occurred. *This may contain personally identifiable data.* Examples are anything you have entered into a form at the time of the error, and any data stored in the session.

Collect specific identifiable data : In addition to basic and context error data, this will allow us to collect specific data about this system. We may use this information to contact you in order to get more information about the error, or to notify you of an update that fixes the error. *This, of course, will contain personally identifiable data.* We will collect your server's IP address and name, and any other data you choose to give us in the provided fields. (All contact fields are optional.)

7.10 About

The About screen (shown in figure 7.15 on the next page reveals which version of the FrontDoor software and database your system is using. Our Technical Support department will want to know this information before they help you diagnose any problems you may be having.

FIGURE 7.15: Main Menu : Server Setup : About


Main Menu / About
Release Version: 6.0.0 Build 98
Database Version: 5.5.0
FrontDoor, Tightrope, and the Tightrope logo are copyright 2015, Tightrope Media Systems.
For more information about FrontDoor or other products from Tightrope Media Systems, please visit
www.trms.com
This software is licensed under the Tightrope Media Systems End-User Software License Agreement.

III. Appendix

Appendix A Access Rights Reference

A.1 Access Rights In FrontDoor

FrontDoor only has two Access Rights: Server Setup and User Management.

A.1.1 Server Setup

Allows access into the **Server Setup** areas in FrontDoor. Users with this Access Right will be able to modify server settings that affect the entire system.

A.1.2 User Management

Allows access to create, modify, and delete Users and Roles in FrontDoor.

A.2 Access Rights In Carousel

Carousel has several Access Rights that can be granted to users of the system. The Access Rights below are grouped by the areas in the software to which they apply. For details, please see *Carousel: The Manual*.

A.2.1 Create - Standard Bulletins

Allows users to create standard bulletins, based on templates.

A.2.2 Create - Uploaded Bulletins

Allows users to upload content to act as a bulletin. Users can upload Flash, Powerpoint, video files, image files, and packages of existing bulletins, assuming that the system is licensed appropriately.

A.2.3 Create - Dynamic Bulletins

Allows users to create dynamic bulletins, including Clock bulletins, Weather bulletins, CableDisplay bulletins, RSS bulletins, Event Schedule bulletins, Interactive bulletins (also requires "Create - Interactive Bulletins" rights), or Live Video Feed bulletins, assuming that the system is licensed appropriately.

A.2.4 Create - Interactive Bulletins

Allows users to create interactive bulletins on a zone, assuming that the system is licensed appropriately. Users will also need the "Create - Dynamic Bulletins" access right assigned to them for the appropriate zone.

A.2.5 Create - Alert Bulletins

Allows users to create Alert bulletins, which interrupt all other bulletins currently running on a Zone.

A.2.6 Create - Repeating Bulletins

Allows users to create bulletins that repeat on an interval. For example, a repeat bulletin with an interval of 4 will be shown after every 4th bulletin.

A.2.7 Create - Set Extra Bulletin Properties

Bulletins can have extra properties that control duration, transitions, sounds, etc. This Access Right allows users to access these properties.

A.2.8 Create - Submit Bulletins to this Zone

Allows users to copy existing bulletins from other zones to this zone.

A.2.9 Create - Template Quick Edit

When creating a bulletin, users with this Access Right are allowed to alter the template used to generate the bulletin. The alteration affects the current bulletin only, leaving the system template untouched.

A.2.10 Create - Auto Authorize Bulletins

Users with this Access Right have their bulletins automatically activated. Without this Right, any bulletins a user creates will be held for approval.

A.2.11 Manage - All Bulletins

Allows users to reorder and delete all bulletins on a zone. To edit bulletins, users will need to also have the corresponding "Create" access right.

A.2.12 Manage - Approve Waiting Bulletins

Users with this Access Right will be able to activate bulletins that are being held for approval.

A.2.13 Manage - Bulletin Housekeeping

Allows users to delete large sections of bulletins at once.

A.2.14 Manage - Other User Bulletins

Allows users to alter bulletins belonging to other users.

A.2.15 Media - Manage User Media

Allows users to upload, manage, and delete their own set of media.

A.2.16 Media - Manage Zone Media

Allows users to upload, manage, and delete media that belongs to the entire zone.

A.2.17 Media - Edit Bulletin Templates

Allows users to alter the templates on a zone.

A.2.18 Setup - Zone Setup

Allows users to make changes to zone settings (linked on the main menu).

A.2.19 Setup - Global System Configuration

Allows users to make changes to system settings (accessed by the **Configure** button on the main menu).

A.2.20 Other - Extras

Allows users to access the Extras menu item. Includes links to RSS feeds, screen saver client downloads, and public web site links.

A.2.21 Other - Edit EventDisplay Schedule

If licensed, allows users to edit the EventDisplay schedule.

A.3 Access Rights In Cablecast

Cablecast has a handful of Access Rights which allow you to limit what functionality your users can have.

A.3.1 Modify Schedule (Location or Channel based)

Allows users to alter the schedule for a single channel, or for every channel at a location (based on domain). Every user can view schedules, this access right allows users to modify a schedule.

A.3.2 Modify Crawl Schedule (Location or Channel based)

Allows users to alter the schedule of crawls for a single channel, or for every channel at a location (based on domain). Every user can view crawl schedules, this access right allows users to modify a crawl schedule.

A.3.3 Modify Shows (Location based)

Allows users to alter show records for all shows at a location. Every user can view a show record, this access right allows users to modify a show record.

A.3.4 Autopilot Force (Location based)

Allows users to force events on devices for a specific location.

A.3.5 Autopilot Send (Location based)

Allows users to send autopilot on a location.

A.3.6 Modify Location Settings (Location based)

Allows users to change settings for a specific location

A.3.7 Modify System Settings (Global)

Allows users to alter the system settings, regardless of location or channel.

A.3.8 Plugin Access (Global)

Allows users to access Cablecast plugins, regardless of location or channel.

A.3.9 Reporting Access (Global)

Allows users to run and view reports, regardless of location or channel.

A.3.10 Batch Functions (Location based)

Allows users to execute batch operations on a location. Includes creating or deleting show and schedule data en masse.

Appendix B Active Directory Integration

FrontDoor 5.3 and higher has support to use your Active Directory (AD) user list. This will allow you to control who can log into Carousel from your domain controller. The AD integration allows general control over who can log into the system, then FrontDoor allows you to further refine that control with our role based permissions system.

We use ASP.NET forms-based authentication with custom AD authentication in the background, instead of IIS's built-in NT Integrated Authentication. We do this because the IIS Integrated only works if you are using Internet Explorer on a Windows machine. With the forms-based authentication we can still use the domain to authenticate users, but are also compatible with all web browsers and platforms. Since forms-based authentication uses cleartext passwords, to increase security you can install a SSL certificate on the web server and run HTTPS.

B.1 Overview of Setup

This integration is only supported on a Carousel server running Windows Server 2003 or 2008, such as a Carousel Pro.

To enable AD integration we will have to change the following .config files. This will tell FrontDoor what domain we are using and how to authenticate users. Then we will have to create an AD group for Carousel user and administrators.

- Join the Carousel server to the domain.
- Run the web server and application pool as a user account that can query the domain controller
- Create Active Directory groups and add users on the domain controller
- Modify the TRMS\Web\FrontDoor\Web.config file
- Log into FrontDoor

B.2 Join the Carousel server to the domain

The Carousel server must be joined to the domain in order for AD integration to work. Join the Carousel server to the domain using an account with access rights to read ActiveDirectory information, read/write on the local server, and communicate over the network.

B.3 Run the web server and application pool as a user account

We need to run the web server or the application pool as an account that can query the domain controller.

If the Carousel server is running Windows 2003 or 2008, we will need to run the application pool as a user account that can query the domain controller. To do

this go the the IIS management screen. Get properties on the application pool that FrontDoor and Carousel are running under. Click the **Identity** tab, select the **Configurable** radio button under the **Application pool identity**, enter the domain account credentials you wish to use.

You may need to add this account to the"IIS_WPG" Group to allow the Worker Process to run under this new account.

If the Carousel server is running Windows XP we will need to run the web server under a user account that can query the domain controller. To do this go the the IIS management screen. Get properties on the **Default Web Site**, click the **Directory Security** tab, click the **Edit...** button in the **Anonymous access and authentication control**, enter the domain account credentials you wish to use in the **Anonymous access** section.

Tightrope does not support Windows XP and AD integration on the server side. For an end user to get official support, they must run the Carousel server software on Windows 2003 or 2008.

B.4 Create Active Directory groups

Now we can log into the domain controller and create two groups:

- TRMS_Users
- TRMS_Admins

ALL users with Carousel access will go into the TRMS_Users group. These users will not be able to administer FrontDoor. Users that are members of the TRMS_Admins group will be allowed to change user roles (FrontDoor User Management rights).

At this time, both groups are hard coded into our software. You will need to use these exact names for the integration to work correctly, including capitalization.

B.5 Modify the FrontDoor Web.config file

We need to change a few of the keys in the FrontDoor .config file. Remember, if you are upgrading from an earlier version of the software (FrontDoor 5.2 or earlier) you will need to copy TRMS\Web\FrontDoor\Web.config.latest over TRMS\Web\FrontDoor\Web.config to get the newest keys.

Edit the following line's **connectionString** property and enter our domain information:

<add name="ADConnectionString" connectionString="LDAP://ad.mydomain.com" />

Change the membership from **<membership defaultProvider="TrmsMembershipProvider">** to **<membership defaultProvider="ADMembershipProvider">**

Uncomment the following section to add the **ADMembershipProvider** key. Update the **connectionUsername** and **connectionPassword** fields to the domain account credentials that we used to run the web server in the step above.

<add name="ADMembershipProvider" connectionStringName="ADConnectionString" applicationName="/FrontDoor" connectionUsername="test@mydomain.com" connectionPassword="1234" connectionProtection="Secure" enableSearchMethods="true" type="System.Web.Security.ActiveDirectoryMembershipProvider" />

B.6 Modify the Carousel Web.config file

We also need to change a few of the keys in the Carousel .config file. These are the same steps as the section above. Remember, if you are upgrading from an earlier version of the software (FrontDoor 5.2 or earlier) you will need to copy TRMS\Web\Carousel\Web.config.latest over TRMS\Web\Carousel\Web.config to get the newest keys.

Edit the following line's **connectionString** property and enter our domain information:

<add name="ADConnectionString" connectionString="LDAP://ad.mydomain.com" />

Change the membership from **<membership defaultProvider="TrmsMembershipProvider">** to **<membership defaultProvider="ADMembershipProvider">**

Uncomment the following section to add the **ADMembershipProvider** key. Update the **connectionUsername** and **connectionPassword** fields to the domain account credentials that we used to run the web server in the step above.

<add name="ADMembershipProvider" connectionStringName="ADConnectionString" applicationName="/FrontDoor" connectionUsername="test@mydomain.com" connectionPassword="1234" connectionProtection="Secure" enableSearchMethods="true" type="System.Web.Security.ActiveDirectoryMembershipProvider" />

B.7 Log into FrontDoor

Now we can log into FrontDoor with one of the domain user accounts that we put in the TRMS_Admins group and start setting up roles for our users to give them access to Carousel.

We will use the standard domain username: **user@mydomain.com** as our username in FrontDoor.

B.8 Notes on how we integrate with Active Directory

When FrontDoor authenticates using AD it enumerates all the users in the TRMS_Users and TRMS_Admins groups. There are several fields that FrontDoor requires to be set on all of the users. If you expirience problems with AD integration, ensure that all the users have the fields below populated.

- Distinguished Name
- UserPrincipalName
- Given
- SN

FrontDoor is pulling the user's First name and Last name from Active Directory using the **givenName** and **sn** fields. All users in TRMS_Users and TRMS_Admins (AD User Groups) must have the First and Last Name (givenName and sn) populated.

By default, users log into FrontDoor using their UserPrincipalName, such as "bob.johnson@mydomain.com". If you would prefer, you can set FrontDoor to use the SAMAccountName. To enable this, add **attributeMapUsername="sAMAccountName"** to the ADMembershipProvider section in the FrontDoor web.config file.

If your setup requires it, add the following two lines to the TRMS\Web\FrontDoor\web.config file in the ADMembershipProvider section:

minRequiredPasswordLength="8"

minRequiredNonalphanumericCharacters="0"

Appendix C Network Ports

Tightrope Media Systems' products use a variety of network ports to communicate with one another. Below you'll find a list of outgoing and incoming ports that are needed for FrontDoor, Carousel, and Cablecast.

C.1 Outgoing Ports

These are ports where the server needs to contact a service outside of itself.

UDP 123: All Tightrope Servers - NTP Time Synchronization.

TCP 80: All Tightrope Servers - Windows Update, Carousel Dynamic Bulletins.

TCP 25: Carousel - Email for Carousel notification (server must allow relaying).

C.2 Incoming Ports

These are ports where the server may need to be contacted from another system.

ICMP v4: All Tightrope Servers - Allows Tightrope systems to *ping* one another for health reasons.

TCP 80: Carousel, Cablecast - The FrontDoor user interface, dynamic output from Carousel or Cablecast (ie: RSS).

TCP 56700: Cablecast - CablecastDeviceControl communication between Cablecast servers and other Cablecast systems.

TCP 56770: Cablecast - SXHwControl communication between SX video servers and Cablecast servers.

TCP 56904: Cablecast - CablecastDSK communication between Cablecast servers and CablecastDSK systems.

TCP 56901: Carousel - Data communication between Carousel servers and Carousel players.

TCP 56902: Carousel - Display status communication between Carousel servers and Carousel players.

TCP 56906: Carousel - Remote commands for Carousel RDA control.

TCP 56907: Carousel - Remote event notification between Carousel servers and Carousel players.

TCP 56908: Carousel - Web socket communication between Carousel servers and Carousel players.

Appendix D Troubleshooting

This chapter will answer some common questions that may arise when using FrontDoor.

D.1 Why can't my users can't log in?

First, double check that they have a user account in FrontDoor. Assuming that they do, make sure they are using the correct user name when they are logging in. If they are, then there is a possibility that their account has become locked. After 5 failed login attempts within 10 minutes, FrontDoor will automatically lock the account to prevent nefarious people from attempting to guess passwords and break into the system. To check if an account is locked, navigate to the User Accounts screen (**Main Menu : User Management : User Accounts**) and look for the troubled account. If the account has been locked, it will be highlighted in red. To unlock the account, click on the **Edit User** link, and on the following screen click the **Unlock User** button. See section 5.5.4 on page 37 for details.

D.2 I can't log in with the Admin account

The Admin account's username is always "`admin`". If you have either forgotten the Admin account password, or suspect it has become locked, please contact Tightrope Media Systems Technical Support. We will be happy to help you reset your password. For contact information, please see section 1.2 on page 7

D.3 Why can't my users access Cablecast?

To access Cablecast with any given user account, that account must be given at least one Cablecast role. If no Cablecast roles are specified for that account, they will not be able to access Cablecast. See section 4.2.1 on page 21 for details.

D.4 Why can't my users access Carousel?

To access Carousel with any given user account, that account must be given at least one Carousel role. If no Carousel roles are specified for that account, they will not be able to access Carousel. See section 4.1.1 on page 19 for details.

D.5 My server's time drifts.

FrontDoor provides several time synchronization techniques to keep your server on time. For detailed instructions on setting up your FrontDoor server to use time synchronization, see section 7.5 on page 50.

A list of publicly available time servers can be found at http://support.microsoft.com/kb/262680.

D.6 I don't have access to an email server.

Google's Gmail[1] service provides a free email account. You can configure FrontDoor to use Google's server by creating a Gmail account and using the following configuration in **Main Menu : Server Setup : Mail Settings** (see section 7.4 on page 48).

Smtp Mail Server : smtp.googlemail.com

Port : 587

Use Authentication : Yes

Enable SSL : Yes

Username : <YourUserName>@gmail.com

Password : <YourPassword>

[1] http://mail.google.com

Appendix E Release History

Tightrope makes frequent revisions to FrontDoor. Below is a detailed list of those changes from the beginning of this release.

E.1 Frontdoor 6.0.0 Release Notes

Story 9131 : Updated Login Page The login screen has been restyled and modernized.

Story 9139 : Updated User Interface The user interface has been restyled and modernized.

Story 9150 : FrontDoor Main Menu is Skipped if the User Only Has Permission for One Product If the user has permission to access Carousel or Cablecast only, the FrontDoor main menu will be skipped, and user will be brought to the main menu of Carousel or Cablecast respectively. The user will be brought to the FrontDoor main menu if there are permissions granted for both Carousel and Cablecast.